TEMAT NUMERU:

Prewencja szkodowa w chmurach

Internet rzeczy – nie jest od rzeczy

Nie taki wybuch straszny

Ryzyko moralne

Socjotechnika wrogiem pracownika

IN THIS ISSUE:

Loss prevention in the clouds

Internet Of Things – why is it a thing?

Outburst – not as black as it is painted

Moral hazard

Social engineering - the employee's enemy

risk focus

ERGO HESTIA

ERGO Hestia Group
1/2019

ERGO HESTIA®

ergohestia.pl

Drodzy Czytelnicy,

świat pędzi jak francuski TGV czy japoński Shinkansen. Wszystko zmienia się błyskawicznie. Jeszcze niedawno w języku biznesowym e-mail, e-learning czy aplikacja mobilna stanowiły dowód nowoczesności firmy. Dzisiaj firmy sięgają głębiej, wydobywając na światło dzienne takie pojęcia, jak big data, sztuczna inteligencja, robotyzacja, uczenie się maszyn czy drukowanie 3D. Jest jeszcze Internet rzeczy (z ang. Internet of Things – IoT), technologia postrzegana przez wielu jako narzędzie, które zrewolucjonizuje czynności domowe i operacje biznesowe. Nazwa Internet rzeczy jest trochę myląca, w rzeczywistości jest to bowiem Internet danych, które stanowią prawdziwą wartość dla każdego użytkownika. Technologia ta stanowi nowe szanse i możliwości rozwoju, również dla rynku ubezpieczeń. Rozwiązania IoT, pozwalające na wykrywanie lub przewidywanie niepożądanych zjawisk, są nie lada wyzwaniem nawet dla najbardziej innowacyjnych firm. W niniejszym numerze „Risk Focus" znajdą Państwo artykuły poświęcone tym zagadnieniom. Gorąco zachęcam również do sięgnięcia do innych tekstów, w których czysta wiedza przeplata się z doświadczeniem ich autorów – ekspertów ERGO Hestii.

Zbigniew Żyra
Redaktor naczelny

Dear Readers,

the world nowadays dashes at the speed of a French TGV train or Japanese Shinkansen (bullet train). Everything changes in the blink of an eye. E-mail communication, online learning or using mobile applications was, until recently, a proof of company's modern style. Today, companies crave for more, bringing to light such concepts as big data, artificial intelligence, robotics, machine learning and 3D printing. And there comes also the IoT (Internet of Things), a technology perceived by many as a tool that will revolutionise household activities as well as business operations. The name itself - Internet of Things - is a bit misleading, as it is in fact Internet of data taht carries real value to every user. The IoT technology opens up new opportunities and brings possibilities development possibilities also for the insurance market. IoT solutions that allow detection or prediction of undesirable phenomena are a challenge, even to the most innovative companies. This issue of "Risk Focus" tackles the matter thoroughly. I also strongly encourage you to reach for other texts which share base knowledge intertwined with the experience of their authors - the ERGO Hestia experts.

Sincerely,
Zbigniew Żyra

risk focus

REDAKTOR NACZELNY / **EDITOR-IN-CHIEF:**
Zbigniew Żyra

ZESPÓŁ REDAKCYJNY / **EDITORIAL TEAM:**
Izabela Balcerzak,
Magdalena Pukownik,
Hubert Rutkowski, Kamil Bara,
Jacek Woronkiewicz,
Tomasz Tkaczyk

ADRES / **ADDRESS:**
ul. Hestii 1, 81-731 Sopot
tel. (58) 555 62 27

E-MAIL / **E-MAIL:** risk.focus@ergohestia.pl
www.ergohestia.pl

PRODUKCJA / **PRODUCTION:**
Skivak Content Experience Sp. z o.o.

KOORDYNATOR PROJEKTU / **PROJECT COORDINATOR:**
Emilia Seweryn

PROJEKT I SKŁAD / **PROJECT AND LAYOUT:**
Bogusław Kalwala

KOREKTA / **PROOF-READING:**
Adam Horowski

risk focus

ERGO HESTIA

ERGO Hestia Group magazine
1/2019

Auta w ogniu

Zarząd portów Genui poinformował o pożarze kilkuset nowych aut Maserati zaparkowanych we włoskiej Savonie. Luksusowe pojazdy były przeznaczone na eksport do krajów Bliskiego Wschodu. W pożarze uszkodzonych zostało również kilka tysięcy samochodów ciężarowych i osobowych o mniejszej wartości niż Maserati. Ogień pojawił się po zalaniu portu w czasie powodzi. Słona woda morska doprowadziła do zwarcia akumulatorów samochodowych, powodując ich eksplozję. Walka strażaków z żywiołem trwała prawie dobę. W wyniku powodzi zniszczeniu uległo także portowe nabrzeże. Strat nie oszacowano.

Luxury cars on fire

The management of the Genoa Port in Italy announced that several hundreds of brand new Maserati cars, parked in Savona, were damaged and lost in a fire. The vehicles were meant for export to the Middle East. Another several thousand trucks and cars of lesser value were also damaged by the fire. The fire first appeared after the port had been flooded. The salt water caused short-circuits in car batteries, which in result led to their explosions. The firefighters fought the fire for almost 24 hours. Also, as a result of the flood, the port quay was destroyed. The loss has not been estimated.

Profil zaufany?

W ostatnim czasie widoczna jest wzmożona aktywność cyberprzestępców, którzy rozsyłają wiadomości z zainfekowanymi załącznikami, podszywając się pod Profil Zaufany, ZUS, KRUK. W każdym z przypadków otworzenie załącznika powoduje zainstalowanie programu, który daje oszustom pełną kontrolę nad urządzeniem. Wiadomości zachowują stylistykę korespondencji powyższych instytucji i wyglądają bardzo wiarygodnie. Zazwyczaj informują o zaległych składkach, płatnościach lub nieopłaconych fakturach, które rzekomo dołączane są do e-maila. Należy pamiętać, aby zawsze weryfikować nadawcę wiadomości oraz nigdy pochopnie nie pobierać i otwierać załączników - zwłaszcza wtedy, gdy nie oczekujemy takiej wiadomości. W przypadku Profilu Zaufanego wiadomości przychodziły z adresu profilzaufanty@gov.pl zamiast profilzaufany@gov.pl.

A Trusted Profile?

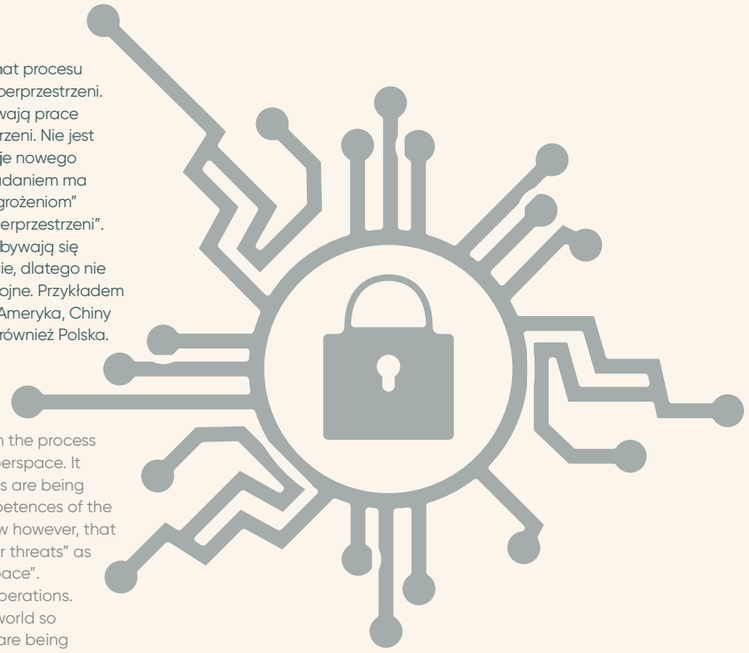
Recently, there has been an increased number of cyber criminals who send messages containing infected attachments, hacking trusted profiles such as health insurance and other institutions. The messages keep the same layout as of the mentioned institutions and thus look very credible. They usually inform about a payment overdue or unpaid invoices that are supposedly attached to the email. In each and every case, opening the attachment will result in installing a program that gives the fraudsters full control over the device. Therefore, remember to verify the sender at all times and never hasten to download or open attachments - especially if you do not expect any such message. In the case of the Trusted Profile, the messages would come from an address containing an error - profilzaufanty@gov.pl instead of profilzaufany@gov.pl.

Polska Cyberarmia

Komisja Obrony Narodowej zorganizowała debatę na temat procesu budowy kwalifikacji i gotowości do działań w obszarze cyberprzestrzeni. Z przedstawionych informacji można się dowiedzieć, że trwają prace koncepcyjne nad powołaniem Wojsk Obrony Cyberprzestrzeni. Nie jest jeszcze znana liczebność, data powołania ani kompetencje nowego rodzaju sił zbrojnych. Wiemy natomiast, że ich głównym zadaniem ma być „wykrywanie, rozpoznawanie i zapobieganie cyberzagrożeniom" oraz „planowanie i prowadzenie działań militarnych w cyberprzestrzeni". Cyberprzestrzeń stała się drugą płaszczyzną, na której odbywają się działania militarne. Cyberwojny miały już miejsce na świecie, dlatego nie powinien dziwić fakt, że powoływane są tego typu siły zbrojne. Przykładem państw, w których takie siły już funkcjonują, są chociażby Ameryka, Chiny i Rosja. Być może do grona państw z cyberarmią dołączy również Polska.

Polish Cyber Army

The National Defense Committee organized a debate on the process of qualifications management and rediness to act in cyberspace. It has been announed that The Cyberspace Defense forces are being conceptualized. The size, appointment date or the competences of the new type of armed forces are not yet known. We do know however, that their main task is to „detect, recognize and prevent cyber threats" as well as „plan and conduct military operations in cyberspace".
The virtual world has become another zone of military operations. Cyberwars have already been taking place around the world so it should not come as a surprise that such armed forces are being appointed. The USA, China and Russia are some of the countries where such forces already exist. Perhaps Poland could also join the group of countries with Cyber Armies.



Woda zniszczyła tamę

Podczas budowy zapory wodnej w południowym Laosie doszło do katastrofy budowlanej. W wyniku zdarzenia życie straciły dwie osoby, kilkaset zostało rannych, a prawie siedem tysięcy straciło dach nad głową. Wskutek zawalenia się części elektrowni 5 mld m^3 wody zalało co najmniej siedem okolicznych wsi położonych nad rzeką Xe-Pian Xe. Pęknięcie konstrukcji było następstwem ulewnych deszczy i burz tropikalnych, jakie w lipcu nawiedziły Laos. Tama miała zostać oddana do użytku jeszcze w 2019 roku, a wartość projektu szacowano na 1,02 mld USD.

Dam destroyed by water

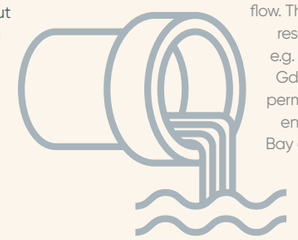
During the construction of the dam in southern Laos, there was a construction disaster. As a result, two persons lost their lives, several hundred were wounded, and almost seven thousand lost their homes. Following the partial collapse of power plant, 5 billion m^3 of water flooded the area of at least seven neighboring villages along the Xe-Pian Xe river. The rupture in the structure was caused by heavy rains and tropical storms that had hit Laos in July. The dam was intended to be opened in 2019, and the value of the project was estimated at USD 1.02 billion.

Ścieki w rzece

W połowie maja 2018 r. doszło do zalania i awarii silników w Przepompowni Ścieków Ołowianka. Instalacja ta odbiera 60% gdańskich ścieków. Aby uniknąć zalania miasta, konieczne było przekierowanie nadmiaru ścieków do rzeki Motławy. Podczas trwającego niemal trzy dni zrzutu, odprowadzano około 2,6 tys. m^3 ścieków na godzinę. Awarię usunięto za pomocą sprowadzonego z Holandii silnika. Urządzenie umożliwiło ponowny start pompy odpowiedzialnej za przepływ odpadów. Badania prowadzone w Zatoce Gdańskiej przez m. in. Instytut Morski w Gdańsku nie wykazały, aby zdarzenie spowodowało trwałe szkody w środowisku.

Sewage leak into the river

In mid-May 2018 there was a flooding and breakdown of the engines of the Sewage Pumping Station in Olowianka, Gdansk. It is responsible for collecting 60% of Gdansk sewage total. In order to avoid the sewage flooding of the city, it was necessary to dispose the excess to Motlava River. During almost three-day pump-out, 2.6 thousand m3 of sewage per hour was dropped. The breakdown was fixed with the help of an engine that came from Holland. The new motor managed to restart the pump responsible for sewage flow. There was an afterwards research completed by e.g. The Marine Institute in Gdansk. It has shown no permanent damage to the environment of Gdansk Bay as a result of the event.

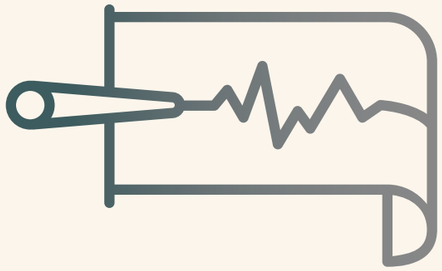


Sposób na trzęsienie ziemi

Budynki w miejscach zagrożonych wstrząsami sejsmicznymi mogą być bezpieczne? Naukowcy z Politechniki Warszawskiej przedstawili pomysł na ich ochronę. Są to tzw. płyny zagęszczane ścinaniem. Praca naukowców zdobyła uznanie na międzynarodowych targach Innotech Expo w Tajwanie. Specjalna substancja, która twardnieje pod wpływem uderzenia lub innego rodzaju gwałtownego nacisku może być wykorzystywana pod budynkami w strefie zagrożonej trzęsieniem ziemi. Płyn jest umieszczany w komorach z tłokami, montowanych w fundamentach budynków. Podczas trzęsienia ziemi wstrząsy poruszają tłokami, których ruchy powodują z kolei zagęszczenie otaczającego je płynu - całość działa jak tłumik. Zawartość antysejsmicznej cieczy tworzą zazwyczaj twarde cząstki tlenków ceramicznych (np. krzemionka) umieszczone w ciekłym organicznym związku chemicznym.

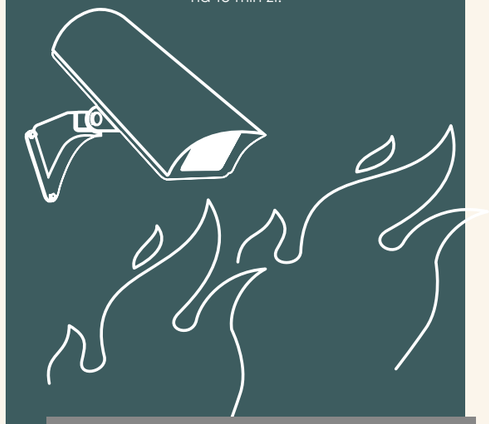
Safety during an earthquake

Can buildings in the seismic-prone zones be safe? Researchers from Warsaw University of Technology have come up with a protection idea - the so-called shear thickening fluids. Their invention has been recognized at the International Innotech Expo in Taiwan.
This special substance that thickens when suddenly hit or pressed may be used under buildings in the earthquake zones. The fluid is placed in the chambers with pistons mounted in the foundations of the buildings. In case of an earthquake, the sudden movement puts the pistons in motion which causes the surrounding fluid to thicken - it all works as a muffler. This fluid is composed of hard particles of ceramic oxides (e.g. silica) placed in a liquid, organic chemical compound.



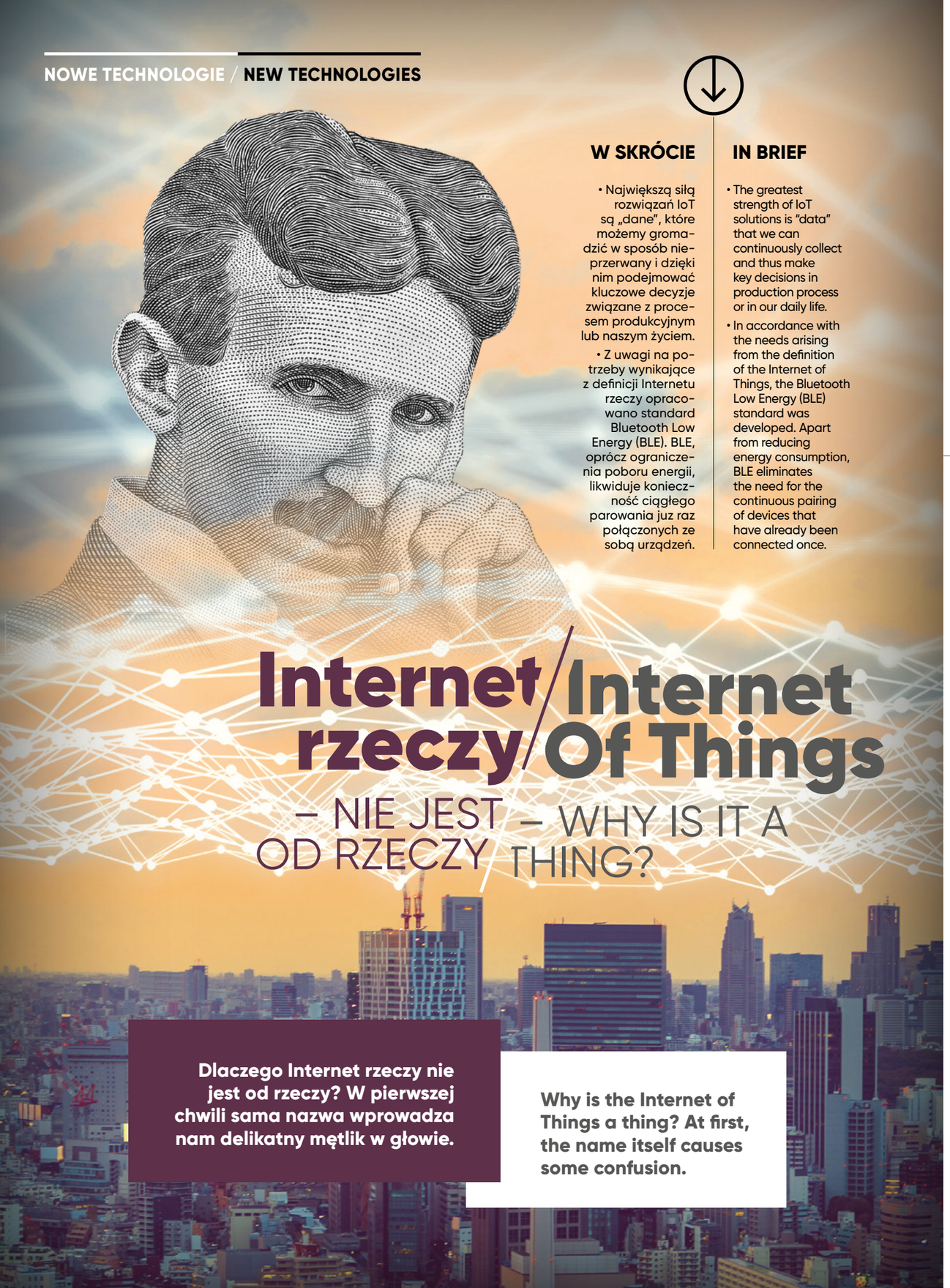
Podpalenie w oku kamery

Kamery telewizji przemysłowej nagrały sprawców podpalenia jednej z firm zlokalizowanej na terenie województwa pomorskiego. Zakład specjalizuje się w usługach stolarskich, malowania proszkowego oraz spawalniczych. Do zdarzenia doszło w trakcie świętowania przez pracowników obchodów 50-lecia przedsiębiorstwa. Pod osłoną nocy włamywacze dostali się do wnętrza firmy, dokonując kradzieży gotówki, a następnie wzniecili ogień w jednym z pomieszczeń produkcyjnych. Pożar rozprzestrzenił się w bardzo krótkim czasie. Gdy na miejsce zdarzenia dotarły pierwsze jednostki Straży Pożarnej, ogień zajmował 3/4 hali o powierzchni ok. 2500 m kwadratowych. Zniszczeniu uległa konstrukcja dachu oraz park maszynowy, znajdujący się wewnątrz hali. Służby ratownicze zdołały odseperować kotłownię gazową, nowy oddział stolarni oraz oddział laserów, w którym znajdowały się urządzenia o wartości 6 mln zł. Ostatecznie straty oszacowano na 10 mln zł.



Arson caught on camera

CCTV cameras have recorded the arsonists to one of the company located in Pomorskie Voivodship, dealing with carpentry works, powder painting and welding services. The event occurred while the employees were celebrating the company's 50th anniversary. The arsonists broke into the company at night, they stole money and then put fire to one of the wine cellar. The fire spread immediately. When the fire brigade reached the destination, ¾ of the 2500 m2 of the place had been already on fire. The fire had destroyed the roof construction and the machinery park indoor. The firemen managed to separate the gas chamber, the new carpentry room and the laser department with equipment of 6 mln PLN worth. The final loss was estimated at 10 mln PLN.



Internet rzeczy / Internet Of Things

– NIE JEST OD RZECZY / – WHY IS IT A THING?

Dlaczego Internet rzeczy nie jest od rzeczy? W pierwszej chwili sama nazwa wprowadza nam delikatny mętlik w głowie.

Why is the Internet of Things a thing? At first, the name itself causes some confusion.

W SKRÓCIE

- Największą siłą rozwiązań IoT są „dane", które możemy gromadzić w sposób nieprzerwany i dzięki nim podejmować kluczowe decyzje związane z procesem produkcyjnym lub naszym życiem.
- Z uwagi na potrzeby wynikające z definicji Internetu rzeczy opracowano standard Bluetooth Low Energy (BLE). BLE, oprócz ograniczenia poboru energii, likwiduje konieczność ciągłego parowania juz raz połączonych ze sobą urządzeń.

IN BRIEF

- The greatest strength of IoT solutions is "data" that we can continuously collect and thus make key decisions in production process or in our daily life.
- In accordance with the needs arising from the definition of the Internet of Things, the Bluetooth Low Energy (BLE) standard was developed. Apart from reducing energy consumption, BLE eliminates the need for the continuous pairing of devices that have already been connected once.

Hubert Karpiński

Menedżer Projektu, zajmuje się zarządzaniem projektami związanymi z technologiami Internet od Things na rynku ubezpieczeń. Absolwent Wydziału Elektroniki i Telekomunikacji Akademii Morskiej w Gdyni. W Grupie ERGO Hestia od 2018 r.

Project Manager, managing insurance IoT projects. A graduate of Faculty of Electronics and Telecommunications at Maritime University of Gdynia. In ERGO Hestia Group since 2018.

Marcin Czepczyński

Menedżer Projektu, zajmuje się zagadnieniami związanymi z monitorowaniem ryzyka z wykorzystaniem systemów opartych o technologię Internet of Things. Absolwent Wydziału Elektroniki i Telekomunikacji Akademii Morskiej w Gdyni. W Grupie ERGO Hestia od 2018 r.

Project Manager, dealing with issues related to risk monitoring using IoT technology. A graduate of Faculty of Electronics and Telecommunications at Maritime University of Gdynia. In ERGO Hestia Group since 2018.

Chcąc lepiej zrozumieć ideę Internetu rzeczy, musimy sobie uświadomić, że nie jest ona powiązana z żadnymi rzeczami.

Oczywiście technologia IoT polega na połączeniu urządzeń, rzeczy, w jedną globalną sieć w celu gromadzenia oraz wymiany informacji pomiędzy sobą.

Największą jednak siłą rozwiązań IoT są „dane", które możemy gromadzić w sposób nieprzerwany i dzięki nim podejmować kluczowe decyzje związane z procesem produkcyjnym lub naszym życiem.

To właśnie dlatego często używamy określenia Internet danych zamiast Internet rzeczy.

Idea ta zbliża nas coraz bardziej do wizji, jaką w 1926 roku roztaczał Nikola Tesla w wywiadzie dla magazynu „Colliers" – kiedy łączność bezprzewodowa osiągnie swój szczytowy poziom, cały świat zmieni się w jeden wielki mózg, w którym poszczególne urządzenia będą tworzyć spójną, rytmiczną całość.

Poniższy artykuł jest próbą przybliżenia wszystkim technologii transmisji, które są „sercem" Internetu rzeczy.

Wi-Fi – ciągle aktualne

W zasadzie technologia Wi-Fi rozwija się od niedawna. Od czasów pierwszych cywilizacji (około sześć tysięcy lat temu) z Wi-Fi nie działo się zupełnie nic. Zaledwie od 30 lat zauważamy rozwój technologii bezprzewodowych.

Pierwsza oficjalna wersja Wi-Fi została wydana w 1997 roku pod nazwą IEEE 802.11-1997.

Kolejnym krokiem było pojawienie się standardu 802.11a (częstotliwość pracy 5 GHz) oraz 802.11b (częstotliwość pracy 2,4 GHz).

Oferowane na tamte czasy prędkości transmisji w odniesieniu do dzisiejszych standardów nie były imponujące – standard 802.11g osiągał zawrotne 54 Mb/s.

Dopiero w ciągu ostatnich 10 lat widzimy ogromny wzrost zainteresowania szeroko rozumianą mobilnością.

In order to better understand the idea of the Internet of Things, we must realize that it is not related to any things.

Of course, IoT technology is about connecting devices and things into one global network in order to collect and exchange information between them. However, the greatest strength of IoT solutions is "data" that we can continuously collect and thus make key decisions in production process or in our daily life.

That is why we often use the expression Internet of Data rather than Internet of Things.

This idea brings us closer Nikola Tesla's vision that he expressed in 1926 in an interview for Colliers magazine. He said that when wireless connectivity reaches its peak level, the whole world will change into one big brain, in which individual devices will form a coherent rhythmic whole.

The following article attempts to familiarize you with the transition technologies that are the "heart" of the transmition.

Wi-Fi – still actual

As a matter of fact, Wi-Fi technology has only developed recently. Since the first civilizations (about six thousand years ago) nothing has been done in terms of Wi-Fi. It is only in the last 30 years that the development of wireless technologies has been noticed. The first official version of Wi-Fi was released in 1997 under the name IEEE 802.11-1997.

The next step was the introduction of the 802.11a standard (5GHz operating frequency) and 802.11b (2.4GHz operating frequency).

The transmission speeds offered then were not very impressive if compared to today's standards - the 802.11g standard reached as much as 54 Mb/s.

It is only during the last 10 years that a great interest in

W 2009 roku opublikowano rozszerzenie IEEE 802.11n, które okazało się milowym krokiem w rozwoju komunikacji bezprzewodowej (praca na częstotliwościach 2,4 GHz oraz 5 GHz) – oferowało prędkość transmisji nawet do 600 Mb/s. Kolejne wersje (opisane standardem IEEE 802.11ac) oferują jeszcze więcej – prędkość nawet do 1 Gb/s.
Dla potrzeb IoT zdefiniowano także standardy IEEE 802.11af oraz 802.11ah: w przypadku tych standardów transmisja realizowana jest w paśmie częstotliwości poniżej 1 GHz, a zasięgi osiągają około 1 km. Dzięki takim zasięgom oraz dużym prędkościom transmisji (sięgającym nawet do 2–3 Gb/s), ściągnięcie jednego filmu w jakości Full HD zajmuje kilka sekund.

Bluetooth Low Energy – „niebieski ząb"

Harald Sinozębny, słynny duński władca, przychodząc na świat około 911 roku n.e., nie przypuszczał, że stanie się protoplastą jednej z najważniejszych współczesnych mobilnych technologii dostępowych. Duży wkład w rozwój technologii BL w latach 90. miała firma Ericsson – jeden z twórców wpadł na tę nazwę podczas lektury książki o wikińskim władcy. Przydomek Haralda we współczesnym mu języku brzmiał Blátonn – „niebieski kieł". To już możemy łatwo przetłumaczyć na język angielski: blue tooth.
Skąd zatem wziął się popularny znaczek, wszechobecny w naszych telefonach? Inicjały Haralda Sinozębnego w języku staronordyckim odpowiadają łacińskim literom H.B., co w alfabecie runicznym odpowiadało znakom Hagalaz i Berkanan, które widać poniżej.
Przechodząc od ciekawej historii do czasów teraźniejszych, wielu z nas nie wyobraża sobie codziennego życia bez technologii Bluetooth lub jej odmiany niskoenergetycznej Bluetooth Low Energy.

Dzięki tej technologii możemy:

- **wymieniać lub synchronizować dane między komputerami i urządzeniami obsługującymi technologię Bluetooth;**
- **używać bezprzewodowej klawiatury i myszy z obsługą technologii Bluetooth;**
- **łączyć się bezprzewodowo z drukarkami, zestawami słuchawkowymi, słuchawkami i głośnikami obsługującymi technologię Bluetooth;**
- **udostępniać innym urządzeniom Bluetooth połączenie z internetem.**

Myśląc o potrzebach wynikających z definicji Internetu rzeczy, opracowano standard Bluetooth Low Energy (BLE). Węzły sieci komunikują się w paśmie częstotliwości 2,4 GHz – wykorzystując 40 kanałów radiowych o szerokości 2 MHz. BLE, oprócz ograniczenia poboru energii, likwiduje konieczność ciągłego parowania ze sobą połączonych już raz urządzeń. Nowa generacja kładzie mniejszy nacisk na podtrzymywanie stałego strumienia informacji. Zamiast tego koncentruje się na wysyłaniu mniejszych porcji danych, kiedy jest to potrzebne, a następnie przełącza połączenie w tryb uśpienia – na czas, gdy nie jest ono używane.
Planowany rozwój standardu w kierunku możliwości budowy sieci BLE w topologii „mesh" (połączenie każdego urządzenia wieloma drogami z innymi urządzeniami) spowoduje, że stanie się on prawdziwą konkurencją dla standardu ZigBee.

ZigBee, czyli „cichy taniec pszczoły"

Podczas przygotowywania tego artykułu zastanawiałem się, co ciekawego można napisać o standardzie ZigBee, który od strony praktycznej przez wielu specjalistów uważany jest za najlepszą metodę komunikacji bezprzewodowej stosowanej w systemach IoT.
Jednak niewielu z nas zdaje sobie sprawę, że twórcy tej technologii inspiracji szukali w przyrodzie.
ZigBee – skąd ta nazwa? Bee to po angielsku pszczoła. Uprawiany przez pszczoły, w celach wymiany informacji, cichy taniec jest określany w języku angielskim jako zig–zag. Składając powyższe, otrzymujemy ZigBee.
Charakterystyczne cechy sposobu wymieniania przez pszczoły informacji są niemalże w całości identyczne z ideami przyświecającymi twórcom standardu ZigBee. Są to: brak sztywnej konfiguracji sieci komunikacyjnej, łatwość jej dynamicznej rekonfiguracji, lokalny zasięg, proste sygnały sterujące komunikacją (co wiąże się z wymaganą niewielką przepływnością danych), bezpieczeństwo przesyłanych danych (pszczoły modyfikują swój język, stosując coś

mobility issues can be noticed. In 2009, the IEEE 802.11n extension was published, which turned out to be a milestone in the development of wireless communication (frequencies 2.4 GHz and 5 GHz) – with transmission speeds up to 600 Mb/s. Subsequent versions (described as IEEE 802.11ac standard) offer even more speed - up to 1 Gb/s. IEEE 802.11af and 802.11ah standards have also been adjusted for IoT: in this case, the transmission is at frequency below 1 GHz and ranges up to 1km. Thanks to such coverage and high transmission speeds (reaching even up to 2-3 Gb/s), downloading a complete movie in Full HD takes only a few seconds.

Bluetooth Low Energy

Harald "Bluetooth" Grimmson, the famous Danish ruler born around 911 AD, never thought that he would become the progenitor of one of the most important contemporary mobile access technologies.
A large contribution to the development of BL technology in the 90s was made by Ericsson company - one of the creators came up with this name while reading a book about the Viking ruler. Harald's nickname in his native language was Blátonn, which can easily be translated into English as blue tooth.
Where does the popular sign on our phones come from? The initials of Harald Bluetooth in the Old Norse language corresponds to the Latin letters H.B, which in the runic alphabet correspond to the signs Hagalaz and Berkanan- see above. Moving on, many of us cannot imagine everyday life without Bluetooth technology or its low-energy version - Bluetooth Low Energy.

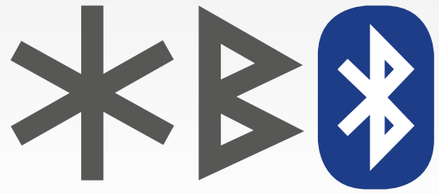
With this technology, we can:

- exchange or synchronize data between computers and devices that support Bluetooth;
- use a wireless keyboard or a mouse with Bluetooth technology;
- connect wirelessly to printers, headsets, headphones and speakers that support Bluetooth;
- share Internet with other Bluetooth devices.

In accordance with the needs arising from the definition of the Internet of Things, the Bluetooth Low Energy (BLE) standard was developed.
The network hubs communicate at the 2.4 GHz frequency - using 40 radio channels with a width of 2 MHz. Apart from reducing energy consumption, BLE eliminates the need for continuous pairing of devices that have already been connected once. This new generation puts less pressure on maintaining a constant stream of information. Instead, it concentrates on sending smaller chunks of data when needed, and then switches the connection to sleep mode when it is not in use.
The planned development of the standard towards the possibility of building a BLE network in the mesh topology (connecting each device in various ways to other devices) will create strong competition for the ZigBee standard.

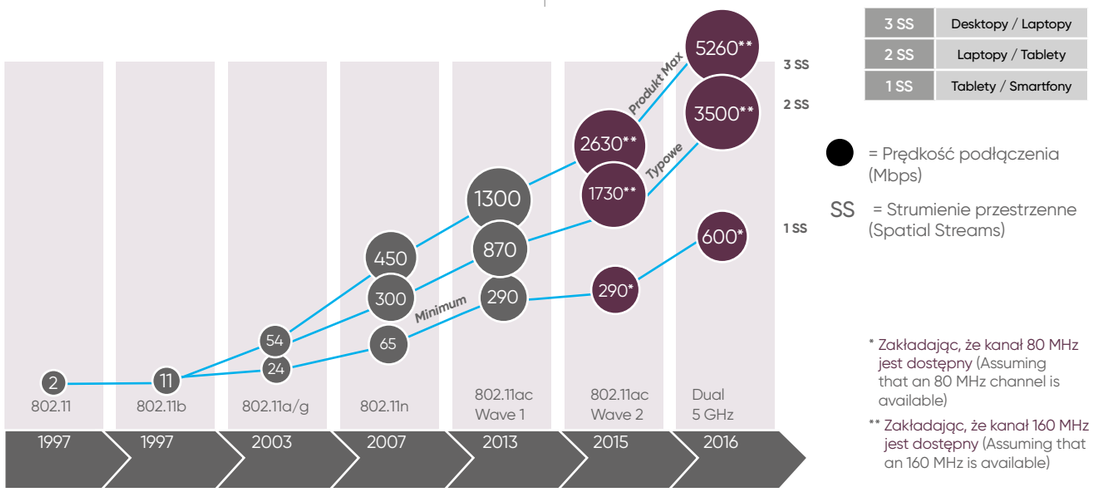
ZigBee - means "silent bee dance"

When writing this article, I was wondering what of interest can be written about the ZigBee standard, which from the practical side is considered by many specialists to be the best method of wireless communication used today in IoT systems. However, there are few of us who realize that the creators of this technology had been looking for inspiration in the nature.
ZigBee - where does the name come from? Bees exchange information by means of a silent dance - that is referred



Rysunek 2. Runy Hagalaz + Berkanan = logo

Figure 2. runes Hagalaz + Berkanan = logo



Rysunek 1. Przykładowa ewolucja dostępnych prędkości w zależności od ilości anten, strumieni przestrzennych i standardu, źródło: cisco.com

Figure 1. Example evolution of available speeds depending on the number of aerials, spatial streams and standards, source: cisco.com

Wydawać by się mogło, że rozwój technologii związanych z IoT odbywa się bez udziału największych operatorów telekomunikacyjnych. Nic bardziej mylnego – najwięksi operatorzy przez lata mocno pracowali nad nowymi technologiami, które będą mogły być wykorzystywane w świecie IoT.

w rodzaju szyfrowania).
To właśnie technologia ZigBee otworzyła drzwi producentom tanich urządzeń przenośnych (z założenia pobierających niewiele energii), które nie wymagają dużych prędkości i dużych zasięgów transmisji danych.
Dziś uważa się, że technologia ZigBee będzie przez najbliższe lata wiodącą technologią w zakresie rozwiązań inteligentnego domu, jak również w przypadku komunikacji M2M (z ang. Machine To Machine). W czerwcu 2017 roku ZigBee Alliance ogłosiło dostępność ZigBee PRO 2017. Standard ten wspiera urządzenia współpracujące ze sobą w ramach ZigBee 3.0.
ZigBee PRO 2017 pozwala producentom budować urządzenia działające w ramach jednej sieci, ale pracujące w różnych pasmach, dzięki czemu lepiej radzą sobie one zarówno z wymaganiami technologicznymi, jak i z wyzwaniami wynikającymi z ich otoczenia. W ramach ZigBee PRO 2017 możemy jednocześnie pracować w dwóch pasmach ISM: 800–900 MHz oraz 2,4 GHz.
Dzięki wskazanym kluczowym przewagom nad konkurencją (większy zasięg, zmniejszony pobór mocy, niskie koszty utrzymania w aplikacjach o małym zapotrzebowaniu na przepustowość), ZigBee jest aktualnie głównym standardem stosowanym w szeroko pojętym Internecie rzeczy.

Sieci komórkowe NB-IoT oraz LTE-M – telekomy w natarciu

Wydawać by się mogło, że rozwój technologii związanych z IoT odbywa się bez udziału największych operatorów telekomunikacyjnych. Nic bardziej mylnego – najwięksi operatorzy przez lata mocno pracowali nad nowymi technologiami, które będą mogły być wykorzystywane w świecie IoT.
Już w 2011 roku, gdy najwięksi krajowi operatorzy rozpoczęli wspólny projekt budowy sieci dostępowej opartej na technologii LTE, wiadomo było, że zrewolucjonizuje ona dotychczasowy model dostępu do usługi internetu mobilnego.
Zaledwie 5 lat później, w 2016 roku, po raz pierwszy w historii ruch w sieci LTE był większy niż ten w sieci 3G. Dzisiaj ciężko wyobrazić sobie sytuację, w której nie mamy możliwości obejrzenia ciekawego filmiku na YouTube czy posłuchania naszej ulubionej muzyki z portalu Spotify. Kolejnym krokiem było powstanie rozwiązań wyspecjalizowanych, opartych o sieć 4G LTE.
W 2016 roku organizacja 3GPP wprowadziła dwa nowe standardy komunikacji: NB-IoT (Narrow Band Internet of Things) oraz LTE-M (Long Term Evolution for Machines). Standardy te łączą w sobie wszystkie cechy, które są utożsamiane z ideą Internetu rzeczy.
Oba standardy funkcjonują w licencjonowanym paśmie i naturalnie rozwijane są przez operatorów, którzy mają już infrastrukturę LTE. Główną zaletą wykorzystywania licencjonowanego pasma jest fakt, iż jest ono wolne od zakłóceń. Na terytorium Polski standard NB-IoT rozwijany jest przez operatora T-Mobile Polska, natomiast standard LTE-M rozwijany jest przez Orange Polska.
Jak sama nazwa wskazuje, NB-IoT to energooszczędna transmisja w wąskim pasmie – 200 kHz, z niską przepustowością (<250 kb/s) oraz opóźnieniami na poziomie pojedynczych sekund. Jednocześnie standard ten zapewnia bardzo dobry zasięg od 5 do 50 km, w zależności od poziomu urbanizacji i przeszkód naturalnych. Wąskopasmowa praca pozwala na dużą koncentrację urządzeń podłączonych w ramach jednej komórki – od 50 do 100 tys. urządzeń.
Znaczącym minusem rozwiązania NB-IoT jest fakt, iż ze względu na długi czas rejestracji urządzenia w sieci przełączanie pomiędzy komórkami powoduje zwiększenie

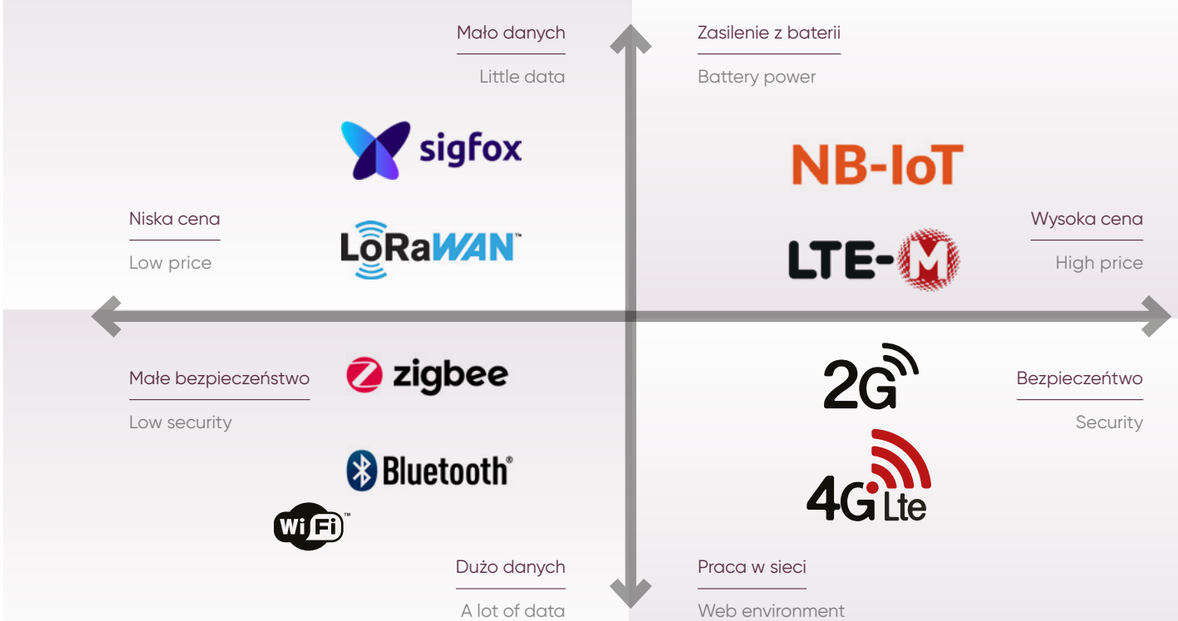
to as a zig-zag. By combining these two terms, we get ZigBee.
The characteristic features of this exchange of information by bees is almost entirely identical to the ideas of the creators of the ZigBee standard. It is the lack of rigid communication network configuration, ease of its dynamic reconfiguration, local coverage, simple signals controlling communication (which is associated with the required low data rate) and security of transmitted data (bees modify their language using something similar to encryption).
ZigBee technology has opened the door for manufacturers of low-cost mobile devices (generally with low power consumption) that do not require high speeds and large data transmission covers.
As of today, it is believed that ZigBee technology will be, for the coming years, the leading technology in the field of smart home solutions as well as M2M (Machine To Machine) communication. In June 2017 ZigBee Alliance announced the availability of ZigBee PRO 2017. This standard supports devices that work together as part of ZigBee 3.0.
ZigBee PRO2017 allows manufacturers to build devices operating within one network but working on different frequencies, thanks to which they cope better with technological requirements as well as surrounding challenges. Within ZigBee PRO 2017, it is possible to simultaneously work on two ISM frequencies: 800-900 MHz and 2.4 GHz.
Thanks to these key competitive advantages (greater coverage, reduced power consumption, low maintenance costs in applications with low bandwidth requirements), as of today, the ZigBee standard is the main standard applicable in the broadly defined Internet of Things.

Mobile networks NB-IoT and LTE-M - telecoms firing back

It would seem that the development of IoT-related technologies is taking place aside from the largest telecommunications operators. Nothing more wrong, as the largest operators have been working hard over the last years on new technologies that can be used in the IoT world.
Already in 2011, when the largest domestic operators started a joint project of building an access network based on LTE technology, it was known that it would revolutionize the existing model of the mobile Internet access.

It would seem that the development of IoT-related technologies is taking place aside from the largest telecommunications operators. Nothing more wrong, as the largest operators have been working hard over the last years on new technologies that can be used in the IoT world.

Only 5 years later, in 2016, for the first time in history, LTE network traffic was larger than that of the 3G network. Today, it is hard to imagine life without being able to watch an interesting YouTube video or listen to our favorite music on Spotify. The next step was the creation of "specialized" solutions based on the 4G LTE network.
In 2016, the 3GPP organization introduced two new communication standards: NB-IoT (Narrow Band Internet of Things) and LTE-M (Long Term Evolution for Machines). These standards combine all the features that are equated with the idea of the Internet of Things.
Both standards operate in a licensed frequency and are naturally developed by operators who already have LTE infrastructure. The main advantage of using a licensed frequency is that it is interference-free. In Poland, the NB-IoT standard is developed by T-Mobile Polska, while the LTE-M standard is developed by Orange Polska.
As the name suggests, NB-IoT is energy-efficient transmission in a low frequency - 200kHz, with low bandwidth (<250kb/s) and delays not more than few seconds. At the same time, this standard provides a very good coverage from 5 to 50 km, depending on the level of urbanization and natural obstacles. Low frequency operation allows a great number of devices to be connected



Rysunek 3. Protokoły komunikacji wykorzystywane w IoT

Figure 3. Communication protocols used in IoT.

poboru mocy. Z tego względu standard ten nie powinien być wykorzystywany w rozwiązaniach mobilnych.
Standard LTE-M wykorzystuje szersze pasmo 1,4 MHz oraz oferuje większą prędkość transmisji – <1 Mb/s. Opóźnienia w porównaniu z NB-IoT są dużo mniejsze – około 10–15 ms.
LTE-M może być wykorzystywany tam, gdzie nie sprawdzają się rozwiązania NB-IoT, czyli w urządzeniach mobilnych (np. w transporcie, gdzie urządzenie musi szybko zmieniać komórki sieci).
Parametrem przemawiającym na niekorzyść LTE-M w stosunku do NB-IoT jest stosunkowo gorsza przenikalność sygnału przez przeszkody.
W zależności od warunków oraz wewnętrznych lub LTE-M mogą pracować przy zasilaniu bateryjnym nawet przez okres 10 lat (bateria około 5 Wh).

Nowi gracze – sieci LPWAN

Natura nie znosi próżni – tym stwierdzeniem możemy określić powstanie rozwiązań spełniających założenia sieci LPWAN (z ang. Low Power Wide Area Network). Do niedawna prym w zakresie komunikacji M2M wiodły sieci telefonii komórkowej. Jednak rozwiązania te często są zbyt kosztowne w implementacji, a szybkość transmisji niepotrzebnie wysoka.
Sieci LPWAN są zoptymalizowane pod kątem niskiego wydatku energetycznego i dużego zasięgu wymaganego w aplikacjach IoT i M2M, a nie szybkości komunikacji. Z tego powodu prędkość przesyłania danych jest niska i wynosi maksymalnie kilkadziesiąt kb/s.
Dwa najpopularniejsze standardy z tej rodziny to Sigfox oraz LoRa.
Standard Sigfox powstał we Francji w 2009 roku.
W Europie sieć Sigfox pracuje w pasmie 868 MHz. Dużym ograniczeniem jest fakt, iż ten typ sieci wymaga budowy własnej infrastruktury technicznej. Alternatywą jest wykorzystanie istniejącej infrastruktury operatorów sieci komórkowych lub publicznej infrastruktury technicznej.
Od strony technicznej transmisja z urządzenia do komórek sieci działa na zasadzie rozgłaszania – w momencie kiedy urządzenie wysyła dane, docierają one do najbliższej stacji bazowej.
Dane transmitowane są do chmury Sigfox, gdzie są agregowane, analizowane i mogą być pobierane do końcowych rozwiązań softwarowych (aplikacje użytkownika).
Podczas działania urządzenia nie jest wymagane utrzymanie stałej łączności z komórką sieci.
Zasięg działania jednej stacji bazowej to nawet 50 km dla otwartych przestrzeni, natomiast w przestrzeni miejskiej od 3 do 10 km.
Kolejnym ograniczeniem sieci Sigfox jest fakt, iż nie nadaje się ona, w odróżnieniu do standardu LoRaWAN, do budowy prywatnych sieci IoT. Natomiast może być wykorzystywana przy budowie rozległych rozwiązań związanych z monitoringiem przestrzeni publicznej (Smart City).
Standard LoRaWAN został opracowany przez firmę

within one cell - from 50 to 100 thousand devices.
A significant downside of the NB-IoT solution is that due to the lengthy device network registration, switching between cells increases the power consumption. Therefore, this standard should not be used for mobile solutions.
The LTE-M standard uses the wider 1.4 MHz frequency, and offers a higher transmission speed - <1Mb/s. Delays compared to NB-IoT are much lower - about 10-15ms.
LTE-M can be used where NB-IoT solutions do not work, i.e. in mobile devices (e.g. transport - where the device must quickly change networks).
A parameter against LTE-M in comparison to NB-IoT is the relatively worse signal transmission due to obstacles.
Depending on conditions and internal settings, devices using the NB-IoT or LTE-M standard can work on battery power for up to 10 years (battery of ar.5Wh).

New players - LPWAN networks

Nature abhors a vacuum – this statement well determines the creation of solutions that meet the objectives of the LPWAN (Low Power Wide Area Network). Until recently, mobile networks were the leaders in M2M communication. However, these solutions are often too expensive to implement and the transmission speed unnecessarily high.
LPWAN networks are optimized for the low power consumption and wide coverage required in IoT and M2M applications, and not for communication speed. Therefore, the data transfer speed is low and amounts to a few dozen kb/s maximum.
The two most popular standards in this family are Sigfox and LoRa.
Sigfox standard was created in France in 2009.
In Europe, Sigfox network operates on the 868 MHz frequency. It is, however, hugely limited as it requires the construction of its own technical infrastructure. An alternative is to use the existing infrastructure of mobile network operators or public technical infrastructure.
From the technical side, the transmission from the device to the network cells works by broadcasting principle - when the device sends data, it reaches the nearest base station.
Data is transmitted to Sigfox cloud, where it is aggregated, analyzed and can be downloaded

Nature abhors a vacuum – it well determines the creation of solutions that meet the objectives of the LPWAN (Low Power Wide Area Network). Until recently, mobile networks were the leaders in M2M communication. However, these solutions are often too expensive to implement and the transmission speed unnecessarily high.

Natura nie znosi próżni – tym stwierdzeniem możemy określić powstanie rozwiązań spełniających założenia sieci LPWAN (z ang. Low Power Wide Area Network). Do niedawna prym w zakresie komunikacji M2M wiodły sieci telefonii komórkowej. Jednak rozwiązania te często są zbyt kosztowne w implementacji, a szybkość transmisji niepotrzebnie wysoka.

Cycleo z Francji. Następnie został nabyty w 2012 roku przez firmę Semtech, która zajmuje się budową interfejsów radiowych dla standardu LoRa.
Obecnie standard ten rozwijany jest przez organizację non-profit LoRa Alliance.
Sieć LoRaWAN w Europie pracuje na częstotliwości 868 MHz. Architektura, podobnie jak w sieci Sigfox, oparta na topologii gwiazdy, w której bramki są pomostami zapewniającymi transmisję pomiędzy urządzeniami końcowymi a serwerem centralnym.
Dużą zaletą w porównaniu z siecią Sigfox jest fakt, iż standard LoRa zapewnia łączność dwukierunkową. Dzięki temu możemy sterować pracą urządzeń oraz wykonywać zdalną aktualizację oprogramowania.
Dodatkowym plusem jest możliwość tworzenia sieci prywatnych i sprawowania nad nimi pełnej kontroli.
Zasięg stacji bazowej w otwartej przestrzeni to 15 km, a w przestrzeni miejskiej od 2 do 5 km.
Największą zaletą jest fakt, iż technologia jest całkowicie otwarta i nie wymaga ponoszenia żadnych opłat abonamentowych związanych z użytkowaniem urządzeń. Standard LoRaWAN jest bardziej elastyczny – dzięki temu możliwy jest rozwój sieci nie tylko przez dużych operatorów telekomunikacyjnych, ale także przez prywatne inicjatywy lub start-upy.

Podsumowanie

Rozwój technologii wydaje się nabierać coraz większego tempa...
Internet rzeczy nie jest już ciekawostką, jaką był jeszcze kilka lat temu. Dzięki gwałtownemu rozwojowi technologii transmisji oraz protokołów komunikacji stał się dobrem, po które każdy z nas może sięgnąć w dowolnym momencie (np. rozwiązania Smart Home, Smart City, Smart Healthcare). Czy za kilka lat wizja Nikoli Tesli stanie się rzeczywistością? Nie wiemy, jednak pewne jest, że świat zmierza w kierunku optymalizacji procesów, większej wydajności lub po prostu oszczędności czasu. Właśnie agregacja i analiza ogromnych ilości danych zbieranych przez rozległe sieci różnego rodzaju sensorów umożliwia nam podejmowanie bardzo precyzyjnych decyzji.
W naszej ocenie rozwój IoT będzie mechanizmem napędowym dla kierunku, który prawie 100 lat temu wyznaczył nam Nikola Tesla. ■

to final software solutions (user applications).
While the device is operating, maintaining constant communication with the network cell is not required.
Each base station can cover up to 50 km for open spaces, and in urban areas from 3 to 10 km.
Another limitation of Sigfox network is that it is not suitable for building private IoT networks, unlike the LoRaWAN standard. However, it can be used in the construction of solutions for public space monitoring (Smart City).
The LoRaWAN standard was developed by the company Cycleo from France. Then the standard was acquired in 2012 by Semtech, which constructs radio interfaces for the LoRa standard.
Currently, this standard is being developed by the LoRa Alliance non-profit organization.
The LoRaWan network in Europe operates at the 868 MHz frequency. The architecture, like in the Sigfox network, is based on a star topology in which the gates are bridges that ensure transmission between the terminal devices and the central server.
A big advantage over Sigfox is the fact that the Lora standard provides two-way communication. Thanks to this, it is possible to control the operation of devices and perform remote software updates. An additional advantage, unlike in Sigfox network, is the possibility of creating private networks and controlling them fully.
The base station in open spaces covers 15 km and in urban areas from 2 to 5 km.
The biggest advantage is that the technology is completely open and does not require any subscription fees related to the devices' usage. The LoRaWan standard is more flexible so it is possible to develop the network not only by large telecommunications operators but also by private initiatives or startups.

Summary

The development of technology seems to be rushing up...
The Internet of Things is no longer the tidbit it was a few years ago. Thanks to the rapid development of transmission technology and communication protocols, it has become a good solution reachable for everyone at any time (e.g. Smart Home, Smart City, Smart Healthcare solutions). Will Nikola Tesla's vision become a reality in a few years? We will see - but certainly the world is moving towards optimization of processes, greater efficiency or simply saving time.
It is the aggregation and analysis of huge amounts of data collected by extensive networks of various types of sensors that enables us to make very precise decisions. In our opinion, the development of IoT will be the driving mechanism in the direction set by Nikola Tesla almost 100 years ago ■

W SKRÓCIE

• Internet rzeczy to zupełnie nowe możliwości w dziedzinie predykcji i prewencji szkodowej. Technologia ta pozwala na ciągły pomiar ryzyka, analizę danych i szybką komunikację, co jest kluczowe w przypadku uniknięcia lub ograniczenia rozmiaru szkody. Niewykorzystanie szansy, jaką dają te rozwiązania, może okazać się grzechem zaniechania.

IN BRIEF

• The Internet of Things offers new possibilities in the field of prediction and loss prevention. This technology allows "continuous risk measurement", data analysis and fast communication, which is crucial to avoid or reduce the size of the damage. If we fail to use the opportunity it offers, it will be an obvious sign of negligence.

Prewencja szkodowa w chmurach

Loss prevention in the clouds

Internet rzeczy (z ang. Internet of Things) to pojęcie, które nie schodzi ostatnio z ust menedżerów i inżynierów reprezentujących różne branże przemysłowe. To sensory, bramki i chmury – cyfrowe chmury pęczniejące od zettabajtów informacji. Wystarczy je odpowiednio „nakłuć", aby z nieba spadł deszcz danych, który może przyczynić się do... no właśnie – czego?

The Internet of Things is a concept that managers and engineers representing various industrial fields have continued to talk about recently. It is sensors, gates and clouds - digital clouds expanding with zettabytes of information. It just takes a little „pinch" for loads of data to pour from the sky, which can contribute to... what exactly?

Zbigniew Żyra

Dyrektor odpowiedzialny za obsługę inżynierską w zakresie prewencji szkodowej. Absolwent Szkoły Głównej Służby Pożarniczej w Warszawie. W Grupie ERGO Hestia od 1994 r.

Director responsible for engineering services in the field of loss prevention. A graduate of the Main School of Fire Service in Warsaw. In ERGO Hestia Group since 1994.

Internet rzeczy (z ang. Internet of Things) to pojęcie, które nie schodzi ostatnio z ust menedżerów i inżynierów reprezentujących różne branże przemysłowe. To sensory, bramki i chmury – cyfrowe chmury pęczniejące od zettabajtów informacji. Wystarczy je odpowiednio „nakłuć", aby z nieba spadł deszcz danych, który może przyczynić się do... no właśnie – czego? Wszystko zależy od oczekiwań. Jedni szukają usprawnień procesów technologicznych, inni podniesienia komfortu pracy czy redukcji kosztów działalności. Moje marzenia obejmują natomiast obszar szeroko pojętej prewencji szkodowej. Straty majątkowe, przestoje w działalności, utrata kontrahentów czy wizerunku to konsekwencje, których chciałby uniknąć każdy przedsiębiorca. Czy technologia IoT może przyczynić się do eliminacji niepożądanych zdarzeń? Z pewnością nie zawsze, ale może zdecydowanie wpłynąć na ograniczenie ryzyka. To szansa, której nie możemy zaprzepaścić.

IoT – internet przyszłości, to zmienia wszystko

Internet rzeczy to nic innego, jak „wielka pajęczyna" łącząca różne przedmioty, które mogą rejestrować, przechowywać i przesyłać między sobą różnego rodzaju informacje. W odniesieniu do przemysłu występuje często pod nazwą IIoT (Industrial Internet of Things), a do samochodów IoV (Internet of Vehicle). Jakiś czas temu pojawiło się również

The Internet of Things is a concept that managers and engineers representing various industrial fields have continued to talk about recently. It is sensors, gates and clouds - digital clouds expanding with zettabytes of information. It just takes a little "pinch" for loads of data to pour from the sky, which can contribute to... what exactly? It all depends on expectations - some are looking for improvements in technological processes, others for improving work comfort or reducing operating costs. On the other hand, my dream relates to the wide area of damage prevention. Property losses, business interruption, contractor outflow or reputational damage are consequences that every entrepreneur would prefer avoiding. Can IoT technology contribute to the elimination of unwanted events? Certainly not always, but it can definitely limit the risk. This is an opportunity we cannot miss.

IoT - the internet of the future, it changes all

The Internet of Things is nothing more than a "large spiderweb" connecting various items that can register, store and send various types of information among each other. In industry, it is often referred to as IIoT (Industrial Internet of Things) and IoV (Internet

Według szacunków International Data Corporation (IDC) obecnie na globalnym rynku znajduje się ok. 10–12 mld „inteligentnych" przedmiotów dysponujących autonomicznym dostępem do sieci, tzn. z własnym, unikalnym adresem IP. Przewiduje się, że do 2020 roku liczba takich urządzeń wzrośnie do blisko 30 mld.

określenie Internet of Everything (Internet wszystkiego czy też Internet wszechrzeczy), które łączy ludzi, przedmioty, procesy i rzeczy.
Według szacunków International Data Corporation (IDC) obecnie na globalnym rynku znajduje się ok. 10–12 mld „inteligentnych" przedmiotów dysponujących autonomicznym dostępem do sieci, tzn. z własnym, unikalnym adresem IP. Przewiduje się, że do 2020 roku liczba takich urządzeń wzrośnie do blisko 30 mld. Będzie to niemal cztery razy więcej, niż wynosi populacja naszego globu. Wkrótce będziemy żyć i pracować w środowisku wysyłających i odbierających sygnały różnych urządzeń. Jeżeli potrafimy wykorzystać big data generowane przez inteligentne urządzenia, to Internet rzeczy stanie się znakiem rozpoznawczym naszej epoki.
Przykładów zastosowań IoT jest wiele. Jednym z najbardziej spektakularnych jest wybudowane kosztem miliardów dolarów koreańskie Songdo – „najbardziej inteligentne miasto świata", miasto naszpikowane milionami sensorów rozmieszczonych w fabrykach, biurowcach, szkołach, na ulicach i w zwykłych domach.
W ślad za miastami przyszłości powstają fabryki przyszłości zgodne z koncepcją Industry 4.0. Gdzieś tam w oddali „majaczy" na horyzoncie idea Loss Prevention 4.0, której fundamentem jest Internet rzeczy.

Różne nosy, różne parametry

Prawdziwym paliwem Internetu rzeczy są dane.
W obszarze zapobiegania szkodom urządzeniami je zbierającymi są różnego rodzaju sensory, które niczym nosy w branży perfumeryjnej czy uszy w muzycznej wychwytują fałszywe nuty. Identyfikują to, czego nie są w stanie zauważyć nasze zmysły, oraz – co najważniejsze – potrafią przesłać informację w miejsca przez nas wskazane. Najczęściej mierzonymi, chociaż nie jedynymi parametrami w obszarze prewencji i predykcji szkodowej w przypadku obiektów przemysłowych, usługowych i magazynowych są temperatura, wilgotność, obecność i drgania. Wszelkie przekroczenia tych parametrów lub niekorzystne korelacje mogą świadczyć o nadchodzącej katastrofie. Jednym z wyjątków jest sensor zalania, który alarmuje po fakcie, np. o wydostaniu się wody z instalacji wodociągowej. Informacja o pojawieniu się wody na posadzce w pomieszczeniu jest jednoznaczna i wystarczająca do podjęcia stosownych działań.

of Vehicles) in relation to cars. The term Internet of All has also appeared recently, connecting people, objects, processes and things.
The International Data Corporation (IDC) has estimated that there are currently globally around 10 - 12 billion "smart" objects with autonomous access to network, i.e. with their own unique IP address. It is predicted that by 2020 the number of such devices will increase to nearly 30 billion. The amount will be almost four times more than the population of our globe. Soon, we will live and work in an environment that sends and receives signals from various devices. If we can make usage of Big Data generated by smart devices, the Internet of Things is to become the hallmark of our era.
There are many examples of IoT applications. One of the most spectacular is the Korean city of Songdo, which construction cost billions of dollars - "the smartest city in the world", it is packed with millions of sensors located in factories, office buildings, schools, streets and "homes". Following the concept of the cities of the future, the factories of the future are created in line with the Industry 4.0 concept. Somewhere in the distance there "looms" the idea of Loss Prevention 4.0, which is based on the Internet of Things.

Different "sensors", various parameters

The real fuel for the Internet of Things is data. In the area of damage prevention, it is sensors that collect various type of data, similarly to the 'nose' in the perfume industry or the "ears" in the music industry, which can pick the "false notes". They identify what our senses are unable to sense and - most importantly - send information to indicated locations. Although there are others, the most frequently measured parameters in loss prevention and prediction in industrial plants, service and storage facilities is temperature, humidity, presence and vibrations. Any excess to these parameters or unfavorable correlations may indicate an upcoming disaster One of the exceptions is the flood sensor, which alerts after the water had been released e.g. from a water supply system. Information about the water on the floor in the rooms is obvious and sufficient enough to take appropriate actions.
It is worth mentioning that registering and transferring

The International Data Corporation (IDC) has estimated that there are currently globally around 10 - 12 billion „smart" objects with autonomous access to network, i.e. with their own unique IP address. It is predicted that by 2020 the number of such devices will increase to nearly 30 billion.

Warto wspomnieć, że rejestracja i przesyłanie danych do chmury oraz ich gromadzenie to połowa sukcesu. Prawdziwym wyzwaniem jest właściwa interpretacja tych informacji, dostrzeżenie niekorzystnych trendów i przygotowanie odpowiednich procedur działania, co jest idealnym polem dla sztucznej inteligencji. Jest więc duża przestrzeń dla takich dyscyplin, jak sztuczna inteligencja, big data czy machine learning.
Nowe rozwiązania technologiczne rodzą się na naszych oczach. W dużej mierze jesteśmy jeszcze w fazie prototypów, prób, błędów i pierwszych wdrożeń lub, jak to powiedział jeden z naszych partnerów biznesowych, „na początku pięknej niekończącej się podróży w nieznany świat IoT, podczas której codziennie odkrywamy coś nowego".

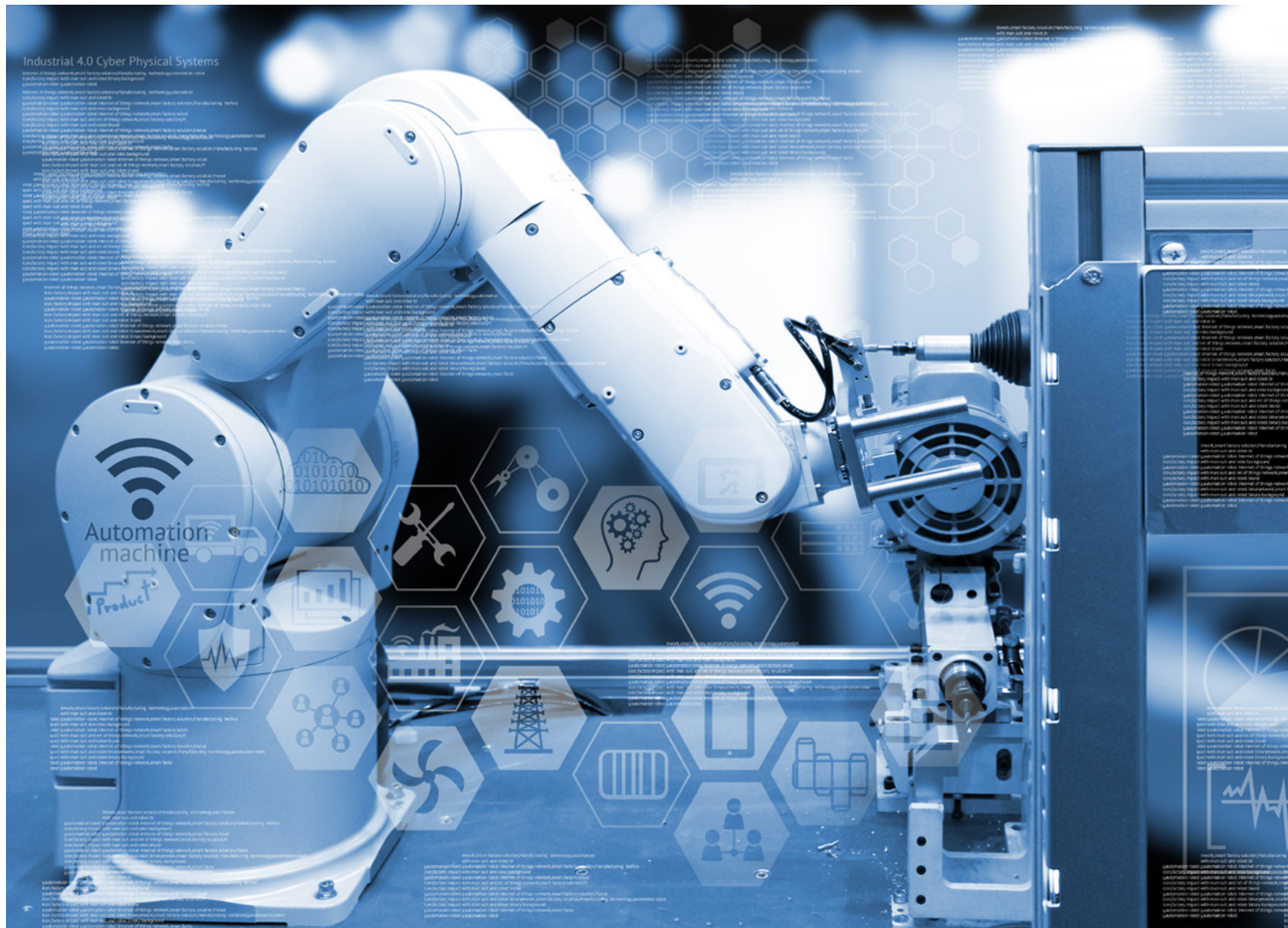
Inteligentny właściciel, inteligentny dom

Smart Home to chyba jedno z pierwszych pojęć, które możemy kojarzyć z Internetem rzeczy. Inteligentne urządzenia domowe pozwalają nie tylko na podniesienie komfortu życia czy realne oszczędności, np. w wyniku mniejszego zużycia energii elektrycznej, ale również, co z mojej perspektywy ma ogromne znaczenie,

data to the cloud and collecting it is only half the success. The real challenge is to have the information interpreted correctly, see unfavorable trends and prepare appropriate operating procedures – all this is an ideal field for artificial intelligence. So there is a lot of room for such disciplines as artificial intelligence, big data or machine learning.
New technological solutions are born just before our eyes. To a large extent, we are still in the phase of prototypes, trials, mistakes and first implementations or, as one of our business partners said, at the beginning of our beautiful, never ending journey into the unknown world of IoT, during which we discover something new every day.

An intelligent owner, a smart home

Smart Home is probably one of the first concepts that we can associate with the Internet of Things. "Smart" home appliances allow not only to increase the comfort of life or real savings, for example as a result of less electricity consumption, but also, which from my perspective is of great importance, increase the level of security of the building. Home sensors can



Technologia IoT pozwala na stworzenie dodatkowej linii ochrony, polegającej na ciągłym monitoringu bez potrzeby „przeciągania" kabli. W przypadku przekroczenia zadanej temperatury powiadamiane są osoby odpowiedzialne za utrzymanie urządzeń elektrycznych.

na zwiększenie poziomu bezpieczeństwa obiektu. Sensory domowe mogą wykrywać niepożądane zjawiska, takie jak dym, tlenek węgla czy woda, a następnie zaalarmować właściciela domu, nawet jeśli znajduje się kilkaset czy kilka tysięcy kilometrów od miejsca zdarzenia. Kilkadziesiąt lat temu takie rozwiązania były wyłącznie w sferze wizji naukowców. Dziś monitorowanie domów za pomocą inteligentnych urządzeń staje się codziennością. Dlatego najwięksi gracze, tacy jak Google, Amazon czy Microsoft, inwestują ogromne pieniądze w rozwój technologii Smart Home. IQ dzisiejszego domu jest dużo wyższe niż domów, które pamiętamy z naszego dzieciństwa. Aż strach pomyśleć, jak bardzo inteligentne będą domy przyszłości.

Rozdzielnice w gorączce

Sprawcami wielu pożarów i w konsekwencji dużych, często wielomilionowych szkód ogniowych i przerw w kontynuacji biznesu są urządzenia i instalacje elektryczne, zwłaszcza rozdzielnice, w których może dochodzić do niekontrolowanego wzrostu temperatury i powstania ognia. Oczywiście można zidentyfikować anomalie termiczne za pomocą kamery termowizyjnej, jednak są to zazwyczaj badania okresowe, których wyniki dotyczą stosunkowo wąskiego przedziału czasowego. Czasochłonność, a co za tym idzie koszty związane z koniecznością zaangażowania profesjonalnego, certyfikowanego specjalisty, w dużej mierze ogranicza możliwość przeprowadzania inspekcji termowizyjnych z dużą częstotliwością. Okresowo przeprowadzane badania termowizyjne są oczywiście niezastąpione i powinny znaleźć się na liście dobrych praktyk z zakresu bezpieczeństwa w każdym zakładzie produkcyjnym i obiekcie usługowym. Jednak technologia IoT pozwala na stworzenie dodatkowej linii ochrony, polegającej na ciągłym monitoringu bez potrzeby „przeciągania" kabli. W przypadku przekroczenia zadanej temperatury powiadamiane są osoby odpowiedzialne za utrzymanie urządzeń elektrycznych. Stosowna reakcja, w wielu przypadkach polegająca na drobnych naprawach typu dokręcenie śrubokrętem, może zapobiec powstaniu poważnego pożaru.

Zamrożone też chronione

Sensory temperatury mogą służyć nie tylko do wykrycia stanu przedpożarowego, ale również roztopowego. Wyobraźmy sobie sklep wyposażony w zamrażarki do przechowywania żywności. Awaria zamrażarki lub brak zasilania (np. w godzinach nocnych) może spowodować rozmrożenie produktów i w konsekwencji konieczność wycofania ich ze sprzedaży. Bez stałego monitoringu temperatury możemy mieć problem z identyfikacją procesu rozmrażania. Sensory IoT mogą błyskawicznie poinformować zainteresowane strony o problemach technicznych. Dzięki uzyskanej w odpowiednim czasie informacji możemy podjąć stosowne działania pozwalające na uratowanie zamrożonej żywności.

Silniki mają drgawki, a niektóre czkawkę

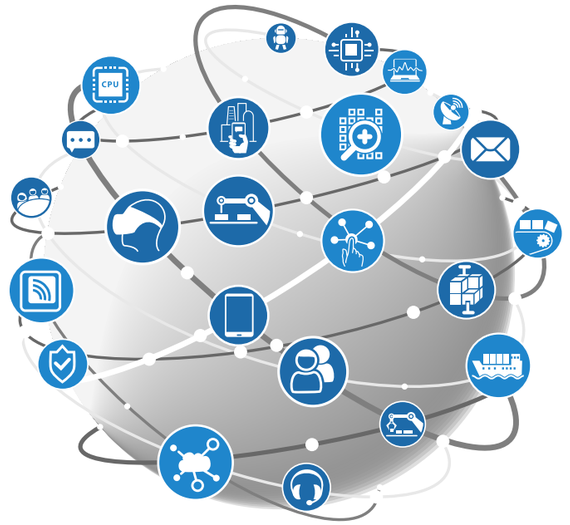
Jednym z niepokojących objawów złego stanu technicznego wielu urządzeń, np. silników, są niewłaściwe, ponadnormatywne drgania. Oczywiście są specjaliści, którzy „słyszą" więcej niż inni, ale zazwyczaj bardziej niezawodna jest stosowana od wielu lat techniczna diagnostyka maszyn i urządzeń. Główne urządzenia technologiczne są często opomiarowane za pomocą różnego typu detektorów kablowych umożliwiających stały monitoring podstawowych parametrów. Powszechnie stosowane są również pomiary za pomocą urządzeń przenośnych. Rozwiązanie to jest stosunkowo łatwe do wdrożenia, jednak obarczone podstawową wadą – cyklicznością. Nie jest to monitoring ciągły, rejestrujący dane z dużą częstotliwością. Do awarii lub innego

IoT technology allows to create an additional protection line based on continuous monitoring, where "dragging" cables is not necessary. If the set temperature is exceeded, persons responsible for the maintenance of electrical devices get notified.

detect undesirable phenomena such as smoke, carbon monoxide or water, and then alert the home-owner, even if they are several hundred or several thousand kilometers from the location. Several decades ago, such solutions were only in the minds of scientists. Today, monitoring homes using "smart" devices is becoming an everyday reality. That is why the biggest players such as Google, Amazon and Microsoft invest huge amounts of money in the development of Smart Home technology. The IQ of today's home is much higher than the homes we remember from our childhood. It's a bit scary to think how "smart" will be the homes of the future.

Electrical Cabinets in a fever

The cause of many fires which often result in multimillion fire damage and business interruption are electrical devices and installations, particularly electrical cabinets, which can lead to uncontrollable temperature rise and formation of fire. Of course, thermal anomalies can be identified using a thermovision camera, but these are usually periodic checks, which show relatively narrow results. They are also time-consuming and costly, due to the need to engage a professional, certified specialist. To a large extent, it limits the ability to carry out frequent thermovision inspections. Periodically carried out thermovision checks are of course irreplaceable and



Bez stałego monitoringu temperatury możemy mieć problem z identyfikacją procesu rozmrażania. Sensory IoT mogą błyskawicznie poinformować zainteresowane strony o problemach technicznych.

Without constant temperature monitoring, we may have a problem with identifying the defrosting process. IoT sensors can instantly inform nterested parties about technical problems.

should be included in the list of good safety practices in every production plant and service facility. However, IoT technology allows to create an additional protection line based on continuous monitoring, where "dragging" cables is not necessary. If the set temperature is exceeded, persons responsible for the maintenance of electrical devices get notified. An appropriate reaction, in many cases involving just minor "screwdriver" repairs, can prevent a serious fire outburst.

Frozen also protected

Temperature sensors can be used not only to detect "pre-fire" status, but also "snowmelt". Imagine a store equipped with food storage freezers. Failure of the freezer or lack of power supply (e.g. at night) may cause de-freezing of the products and, consequently, the need to withdraw the products from sale. Without constant temperature monitoring, we may have a problem with identifying the defrosting process. IoT sensors can instantly inform interested parties about technical problems. Thanks to receiving the information in time, appropriate saving measures can be taken.

Motors may have convulsions and hiccups

One of the disturbing symptoms of poor technical condition of many devices, e.g. motors, is inappropriate, excessive vibrations. Of course, there are specialists who "hear" more than others, but usually the standardized technical diagnostics of machines and devices is more reliable. The main technological devices are often wired with various types of "cable" detectors, enabling constant monitoring of basic parameters. Mobile measuring is also commonly used. The solution is relatively easy to implement, but it has a basic disadvantage – it is cyclic. This is not continuous monitoring that records data at high frequency. A failure or other incident may occur in between measurements. IoT technology provides online monitoring without the need for wiring. This is usually a great solution for small and medium-sized companies that cannot yet afford traditional, extensive systems or larger plants that want to have control over additional machines and devices. IoT sensors installed on motors or other machines record vibrations and send information via appropriate communication protocols to the cloud, where they are properly processed.
Appropriate algorithms and fast processors allow instant

incydentu może dojść w okresie pomiędzy pomiarami. Technologia IoT zapewnia monitoring online bez konieczności stosowania okablowania. Jest to zazwyczaj świetne rozwiązanie dla małych i średnich firm, które dotychczas nie dorobiły się tradycyjnych rozbudowanych systemów, lub większych zakładów decydujących się na kontrolowanie dodatkowych maszyn i urządzeń. Zainstalowane na silnikach lub innych maszynach sensory IoT rejestrują drgania i przesyłają informacje za pomocą odpowiednich protokołów komunikacyjnych do chmury, gdzie następuje ich właściwa obróbka.
Odpowiednie algorytmy i szybkie procesory pozwalają na błyskawiczną analizę otrzymywanych informacji i porównanie ich np. do stanów normatywnych lub występujących w przeszłości stanów przedawaryjnych. Dopiero takie operacje można określić predykcją, czyli przewidywaniem zdarzeń, które mogą wystąpić w bliższej lub dalszej przyszłości. Człowiek nie jest w stanie wykonać tej pracy w takim czasie i z taką dokładnością. Dlatego z pomocą przychodzi sztuczna inteligencja, która poradzi sobie z tonami informacji i milionami scenariuszy. Bez zastosowania zaawansowanych algorytmów duża część otrzymanych informacji jest bezużyteczna. Generowanie wynikającej z niej wiedzy

Appropriate algorithms and fast processors allow instant analysis of received information and comparing it, for example, normative states or "pre-abnormal states" that occured in the past.

analysis of received information and compare them to, for example, normative states or "pre-abnormal states" that occured in the past. These operations can be called predictive as they foresee events that can occur in the near or distant future. A human is not able to do this work in such a time and with such accuracy. That is why artificial intelligence comes in handy when dealing with tons of information and millions of scenarios. Without the use of advanced algorithms, much of the information received is useless. Generating the knowledge resulting from the data processing is the key aspect in the field of prediction.
The saying "we learn from damage" is well known among insurers. In the case of IoT systems, there is a good chance that the lesson from damages will be learned. If the system "notices" an unfavorable trend

Odpowiednie algorytmy i szybkie procesory pozwalają na błyskawiczną analizę otrzymywanych informacji i porównanie ich np. do stanów normatywnych lub występujących w przeszłości stanów przedawaryjnych.

jest kluczowym aspektem w zakresie predykcji. Znane jest wśród ubezpieczycieli powiedzenie, że szkody uczą. W przypadku systemów IoT jest duża szansa, że nauka ze szkód nie pójdzie w las. Jeżeli system zauważy niekorzystny trend, który w przeszłości skutkował np. awarią maszyny, natychmiast powiadamia osoby odpowiedzialne za utrzymanie ruchu. Szybka reakcja może uchronić przedsiębiorstwo przed dużymi stratami materialnymi i długotrwałym przestojem w działalności.

Prewencja przyszłości?

Internet rzeczy to zupełnie nowe możliwości w dziedzinie predykcji i prewencji szkodowej. Technologia ta pozwala na ciągły pomiar ryzyka, analizę danych i szybką komunikację, co jest kluczowe w przypadku uniknięcia lub ograniczenia rozmiaru szkody. Niewykorzystanie szansy, jaką dają te rozwiązania, może okazać się grzechem zaniechania.
Oczywiście obok zalet urządzenia komunikujące się bezprzewodowo mają również swoje wady, takie jak niepewność transmisji czy czas pracy baterii sensorów. Jednak z moich analiz wynika, że dostawcy urządzeń coraz lepiej radzą sobie z tymi słabościami.
Czy jest to rewolucja prewencyjna lub predykcyjna? Z pewnością tak, chociaż ostateczną ocenę wystawią kolejne pokolenia ekspertów i inżynierów ryzyka. Sztuką jest optymalne wykorzystanie technologii IoT, umiejętne lokalizowanie sensorów oraz budowanie skutecznych modeli analitycznych. Do tego niezbędna jest unikalna wiedza, doświadczenie i kreatywność. Jednym słowem, pojawiły się nowe możliwości prewencji i tylko od nas zależy, w jaki sposób uda się je wykorzystać.
Należy jednak pamiętać, że przesłanie sygnału z miejsca A do miejsca B może odbyć się za pomocą kabla, który traktowany jest jako bardziej niezawodny sposób niż łączność bezprzewodowa. Dlatego tradycyjne systemy detekcji, np. pożaru, nadal stanowią podstawę zabezpieczeń obiektów, podobnie jak tryskacze czy inne stałe urządzenia gaśnicze. Rozwiązania IoT są jednak doskonałym uzupełnieniem kompleksowej koncepcji bezpieczeństwa.
Dawniej przewidywaniem przyszłości zajmowały się wróżki. Dzisiaj czarodziejską kulę zastępują sensory, routery, protokoły komunikacyjne, aplikacje, algorytmy i modele predykcyjne. Taka drobna różnica. ■

that in the past resulted, for example, with a machine failure, it immediately notifies those responsible for maintenance. A quick response can save an enterprise from heavy material losses and long-term business interruption.

Prevention of the future?

The Internet of Things offers new possibilities in the field of prediction and loss prevention. This technology allows "continuous risk measurement", data analysis and fast communication, which is crucial to avoid or reduce the size of the damage. If we fail to use the opportunity it offers, it will be an obvious sign of negligence. Of course, despite their advantages, devices that communicate wirelessly also have their disadvantages, such as uncertainty of transmission or sensor battery capacity. However, my analysis shows that device suppliers manage well to cope with these weaknesses.
Is this a preventive or predictive revolution? Certainly yes, although final assessment will be given by the future generations of experts and risk engineers. The trick is to optimally use IoT technology, skillfully locate sensors and build effective analytical models. For this, unique knowledge, experience and creativity is required. Simply, there are new possibilities for prevention that have shown up and it is only up to us how we use them.
However, it should be remembered that the signal from place A to place B can be transmitted via a cable, which is treated as a more reliable way than wireless communication. That is why traditional detection systems, such as for fire, are still the basis for protecting premises, as do sprinklers or other fixed fire extinguishing devices. However, IoT solutions are a perfect complement to the comprehensive security concept.
In the past, fortune-tellers used to predict the future. Today, the magic crystal ball is replaced by sensors, routers, communication protocols, applications, algorithms and predictive models. Just a tiny difference. ■

W SKRÓCIE

- Systemy ochrony przed skutkami wybuchu (prościej nazywane systemami przeciwwybuchowymi) ze względu na zasadę działania możemy podzielić na aktywne i pasywne.
- Technika odciążania wybuchu jest regulowana normą PNEN 14491:2012 dla pyłów oraz normą PN-EN 14994:2009 dla gazów.

IN BRIEF

- Protection systems against the effects of an explosion (i.e.: anti-explosion systems), due to their operational principle can be divided into two types: active and passive.
- The explosion relief technique is regulated by PNEN 14491:2012 for dust and norm PN-EN 14994:2009 for gases.

Nie taki wybuch straszny..

Not such a terrible outburst...

Cz. II – zabezpieczenia przeciwwybuchowe

W nowoczesnym przemyśle mamy do czynienia z różnymi zagrożeniami wynikającymi najczęściej z prowadzonych procesów produkcyjnych. Jednym z istotniejszych ryzyk, jeżeli weźmiemy pod uwagę potencjał szkodowy, jest zagrożenie wybuchem. Jak się chronić?

Part II – explosion protection

In modern industry, we deal with various threats resulting most often from the production processes. In terms of damage potential, one of the most important risks is the danger of explosion. How can we prevent it?

Krzysztof Folga

Inżynier ds. Oceny Ryzka, zajmuje się zagadnieniami ryzyka ogniowego, wybuchowego, utraty zysku oraz uszkodzenia maszyn i urządzeń. Absolwent Wydziału Mechanicznego Politechniki Krakowskiej oraz studiów podyplomowych w zakresie Jakości i BHP. W Grupie ERGO Hestia od 2017 r.

Risk Assessment Expert, dealing with risk issues fire, explosive, loss of profit and damage to machinery and equipment. A graduate of the Faculty of Mechanical Engineering of the Cracow University of Technology and postgraduate studies in the field of Quality and Health and Safety. In the ERGO Hestia Group since 2017.

Co zrobić, kiedy dojdzie do wybuchu?

Jeżeli nie rozpatrywaliśmy wcześniej, sami lub z pomocą specjalistycznej firmy, możliwości wystąpienia zdarzenia wybuchowego i związanych z tym szkód, to w większości przypadków można powiedzieć, że prawdopodobnie już jest za późno. W razie wystąpienia wybuchu, w znakomitej większości przypadków, działanie sprowadza się do opanowania pożaru, który z reguły występuje bezpośrednio po nim. Niszczycielska siła fali ciśnienia spowoduje, znacznie wcześniej niż pożar, straty materialne, które są nieodwracalne. Można jedynie podjąć próbę ratowania przed spaleniem pozostałego mienia. Środki obrotowe będą już zapewne zniszczone przez dym do tego stopnia, że nie będzie można ich zyskownie sprzedać. Do wysokości szkody prawdopodobnie będzie trzeba doliczyć znaczne koszty utylizacji towarów, dlatego najważniejszym działaniem w celu ochrony przed skutkami wybuchu jest montaż certyfikowanych zgodnie z ATEX systemów ochronnych (Dyrektywa 2014/34/UE – Atex 114).

Systemy ochronne aktywne i pasywne

Systemy ochrony przed skutkami wybuchu (prościej nazywane systemami przeciwwybuchowymi) ze względu na zasadę działania możemy podzielić na aktywne i pasywne. Pasywne zabezpieczenia przeciwwybuchowe nie wymagają działania systemów elektrycznych czy elektronicznych, wykorzystują bowiem do funkcjonowania same zjawiska fizyczne, takie jak odpowietrzanie (odciążanie) wybuchu i bezpłomieniowe odciążanie wybuchu. Zabezpieczenia aktywne posiadają precyzyjne czujniki analizujące sytuację w sposób ciągły, wysyłające sygnał do centrali systemu, która podejmuje decyzję zadziałania i podaje sygnał do elementów wykonawczych systemu (tłumienie wybuchu).

Zasada działania systemów

Podstawową zasadą każdego systemu ochronnego, aktywnego i pasywnego, jest obniżenie (maksymalnie

What to do when an explosion occurs?

If we have never, neither on our own nor with the assistance of a specialized company, considered the threat of an explosion and the accompanying damage, then in most cases not much can be done - it is probably already too late. In the event of an explosion, the undertaken action mostly narrows down to controlling the fire that usually occurs immediately after the explosion. Much earlier than the fire, the destructive force of the pressure wave will cause irreversible material losses then, you can then only try to save what remains from burning. The current assets would probably be damaged so much by the smoke that they will not give any profit if sold. The damage value would probably have to be increased with high disposal costs of goods. Therefore, the most important action protecting against the effects of an explosion is the use of protection systems, certified in accordance with ATEX (Directive 2014/34/EU - Atex 114).

Active and passive protection systems

Protection systems against the effects of an explosion (i.e.: anti-explosion systems), due to their operational principle can be divided into two types: active and passive. Passive explosion protection does not require the operation of electrical or electronic systems, as it uses only physical phenomena to function, such as venting (relieving) explosion and flameless explosion relief. Active protections uses precise sensors that analyze the situation continuously. They send a signal to the system's central, which then decides whether to operate by sending a signal to the system's actuators (explosion suppression).

Principle of system operation

Whether it be active or passive, the basic principle of each protective system, is to reduce (as fast as possible) the explosion pressure (Pmax) to the level of reduced pressure (Pred). Pred (reduced pressure) should be set at a safe level for the protected device so that the damage does not occur in it. Depending

szybko) ciśnienia wybuchu Pmax do poziomu ciśnienia zredukowanego Pred. Ciśnienie zredukowane Pred powinno być określone na poziomie bezpiecznym dla chronionego aparatu tak, aby nie powstały w nim uszkodzenia. W zależności od wybranego systemu ochrony, jego zadziałanie powinno być zawsze na określonym poziomie: ciśnienie Pstat – statyczne ciśnienie otwarcia (odciążanie, odpowietrzanie wybuchu) lub Pa – ciśnienie aktywacji (tłumienie wybuchu).

Istnieje również sposób ochrony przed skutkami wybuchu oparty na zasadzie projektowania urządzeń odpornych na ciśnienie wybuchu (potocznie nazywanych urządzeniami „na 10 bar", lecz wartość ta nie jest przywołana w żadnej normie) lub odpornych na uderzenie ciśnienia wybuchu. Wbrew pozorom określenia te nie są tożsame. W produkcji urządzeń odpornych na ciśnienie wybuchu nie dopuszcza się pojawienia w nich trwałych odkształceń po wystąpieniu wybuchu, natomiast w drugim rozwiązaniu dopuszcza się natomiast odkształcenia trwałe bez możliwości rozerwania aparatu. Urządzenia te opisuje norma PN-EN 14460:2008. Instalacje takie, ze względu na grubość ścianek, są z reguły ciężkie i kosztowne, niemniej często występują głównie w przemyśle spożywczym i farmaceutycznym, przy produkcji z wykorzystaniem surowców sypkich (proszków organicznych), gdzie podstawowymi operacjami jednostkowymi są: mielenie (na sucho), mieszanie i konfekcjonowanie.

Odciążanie wybuchu

Technika odciążania wybuchu jest regulowana normą PN-EN 14491:2012 dla pyłów oraz normą PN-EN 14994:2009 dla gazów. Najbardziej popularne jest odciążanie wybuchu przez montaż tzw. paneli dekompresyjnych, klap rozrywnych, klap samozamykających, membran itp. To rozwiązanie stosowane jest ze względu na relatywnie niskie koszty zakupu tych urządzeń, ich instalacji oraz szerokiego zastosowania. Istotnymi wadami takiego systemu jest konieczność wyprowadzania na zewnątrz, do bezpiecznej strefy, pozostałości po wybuchu. Są nimi niejednokrotnie palące się, spalone i niespalone cząstki, co często może stanowić zagrożenie pożarowe. Aplikacja systemu odciążania może przysparzać kłopotów w wydzieleniu bezpiecznej przestrzeni, tzw. strefy bezpieczeństwa,

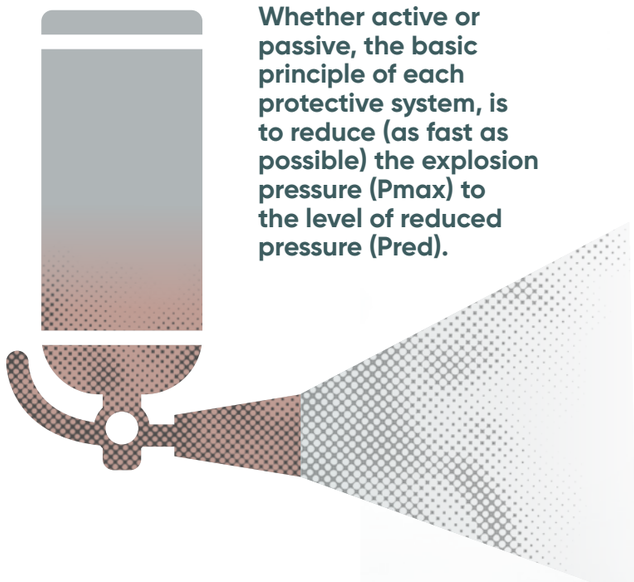
Podstawową zasadą każdego systemu ochronnego, aktywnego i pasywnego, jest obniżenie (maksymalnie szybko) ciśnienia wybuchu Pmax do poziomu ciśnienia zredukowanego Pred.

on the chosen protection system, its operation should always be at a specified level: Pstat pressure - static entry pressure (relieving, venting) or Pa - activation pressure (explosion suppression).

There is also a way to protect against the explosion effects based on the principle of designing devices resistant to explosion pressure (commonly referred to as "10 bar" devices, but this value is not referenced to in any standard) or impact-resistant explosion pressure. Contrary to appearances, the terms are not identical. In the production of devices resistant to explosion pressure, permanent deformation should not happen after the occurrence of an explosion. In the second solution, permanent deformations may happen but no device bursting. These devices are described in the PN-EN 14460:2008 standard. Due to their wall thickness, such devices are usually heavy and expensive, however, they may often be found in the food and pharmaceutical industries, in production involving powered raw materials (organic powders), where the basic unit operations are: grinding (dry), mixing and confectioning.

Explosion relief

The explosion relief technique is regulated by PN-EN 14491:2012 for dust and PN-EN 14994:2009 for gases. The most popular explosion relief is by mounting so-called decompression panels, tear-off flaps, self-closing flaps, membranes, etc. This solution is used due to the relatively low purchase costs of these devices, their installation and the possibility of widespread use. An important disadvantage of such a system is the necessity of moving the remains of an explosion to a safe zone outdoor. These are often burning, burnt and unburned particles, which can often constitute



Whether active or passive, the basic principle of each protective system, is to reduce (as fast as possible) the explosion pressure (Pmax) to the level of reduced pressure (Pred).

W przypadku systemów odciążania istnieje również ryzyko źle wyliczonej powierzchni odciążenia, nieuwzględnienia siły odrzutu (posadowienie aparatu), konieczność montażu deflektorów, zagrożenia dotyczące zjawiska, np. implozji zbiorników.

której zasięg może wynosić do kilkudziesięciu metrów. Następnym istotnym ograniczeniem jest brak możliwości odciążania substancji toksycznych oraz wyprowadzania toksycznych produktów spalania na zewnątrz, do atmosfery. Dobra praktyka inżynierska stanowi również, że nie odciąża się urządzeń i aparatów procesowych wewnątrz budynków i pomieszczeń zamkniętych.

Chociaż nie ma uregulowań prawnych normalizujących tę kwestię, jest to racjonalnie uzasadnione, np. ze względów pożarowych. W przypadku systemów odciążania istnieje również ryzyko źle wyliczonej powierzchni odciążenia, nieuwzględnienia siły odrzutu (posadowienie aparatu), konieczność montażu deflektorów, zagrożenia dotyczące zjawiska, np. implozji zbiorników. Kanały dekompresyjne wyprowadzające skutki wybuchu na zewnątrz budynku powinny być ściśle zaprojektowane zgodnie z normą PN-EN 14491:2012. Nieodpowiednio zaprojektowany kanał dekompresyjny (średnica, długość, kąty załamania) może być przyczyną zwiększenia zredukowanego ciśnienia wybuchu Pred w chronionym aparacie i w konsekwencji jego zniszczenia, pomimo zastosowania systemu ochronnego. Kolejną wadą systemu jest konieczność jego demontażu po zadziałaniu i wymiany elementów na nowe. Istnieją również rozwiązania, które nie posiadają konieczności rozbiórki – są to np. samozamykające klapy odciążające wybuch (głównie dla pyłu węglowego), które po – eksplozji domykane są własnym ciężarem, sprężynowo lub z użyciem poduszki powietrznej i uniemożliwiają dopływ tlenu, co zapobiega wystąpieniu pożaru. Metody te zostały opisane w normie PN-EN 14797:2009.

a fire hazard. The application of the unloading system can be difficult as it requires a separated safe zone, even up to several dozen meters wide. Another important limitation is the lack of possibility to relieve toxic substances and to get the toxic combustible products outdoor, into the atmosphere. Good engineering practice also says that the devices and processing appliances are not to be relieved to the inside of buildings and closed spaces.

Although there are no legal regulations that formalize this issue, it is rationally justified, for example for fire safety reasons. In the case of relieving systems, there is also a risk of a insufficiently calculated relieving area, neglecting the recoil force (foundation of the appliance), the need to install deflectors, risk of events such as e.g. implosion of tanks. Decompression channels discharging effects of the explosion outside the building should be strictly designed in accordance with the PN-EN 14491:2012 standard. An improperly designed decompression channel (diameter, length, refraction angles) can cause the increase in reduced Pred burst pressure in the protected device and consequently cause its destruction, despite the use of a protective system. Another disadvantage of the system is the necessity to dismantle it after activation and the replacement of used elements with new ones. There are also solutions that do not need to be dismantled - these are, for example, self-closing flaps relieving the explosion (mainly for coal dust), which after explosion are closed with their own weight, by a spring or with the use of an air cushion and prevent the supply of oxygen, which prevents the occurrence of fire. These methods are described in PN-EN 14797:2009 standard.

Bezpłomieniowe odciążanie wybuchu

Inną formą odciążania wybuchu jest bezpłomieniowe odciążanie wybuchu. Technika ta opisana jest w normie PN-EN 16009:2011. Podstawową różnicą pomiędzy systemem odciążania a bezpłomieniowym systemem odciążania wybuchu jest to, że skutki – eksplozji, opuszczające chroniony aparat, pozbawione są płomienia, a temperatura gazów wylotowych zostaje obniżona. Urządzenie, najprościej mówiąc, składa się z mechanizmu odciążającego z zamontowanym przerywaczem płomienia i wymiennikiem ciepła. Przerywacz płomienia nie dopuszcza do przeniesienia się ognia z wnętrza chronionego aparatu, a wymiennik ciepła odbiera wysoką temperaturę gazów wylotowych. Urządzenia są stosowane głównie wewnątrz budynków, w sytuacjach, kiedy nie ma możliwości wyprowadzenia skutków wybuchu poza budynek. Niestety posiadają szereg ograniczeń, takich jak np. ściśle określone wymogi w odniesieniu do kubatury pomieszczenia, w którym są zainstalowane, oraz brak możliwość instalowania dla toksycznych produktów spalania. Dodatkowo w przypadku urządzeń bezpłomieniowego odciążania wybuchu, zamontowanych wewnątrz pomieszczenia, należy również wyznaczyć tzw. przestrzeń bezpieczną, sięgającą kilku metrów wokół urządzenia.

Po zadziałaniu – mechanizmu, jak w przypadku zwykłego panelu dekompresyjnego, należy zdemontować system i przywrócić go do pełnej sprawności, montując panele pod urządzeniem bezpłomieniowym. Na rynku dostępny jest również tzw. zawór odciążający wybuch, który rozszerza się w momencie eksplozji, a po – niej następuje samozamknięcie. Zawór taki – często można spotkać na filtrach w układach odpylania.

Tłumienie wybuchu

Kolejnym dostępnym na rynku rozwiązaniem systemu ochronnego jest aktywny system zabezpieczenia przed skutkami wybuchu, tzw. tłumienie wybuchu HRD (High Rate Discharge Bottles). Wymagania co do tego typu systemów zawarte zostały w normie PN-EN 14373:2006. System ten polega na rozproszeniu środka tłumiącego (proszku tłumiącego) wewnątrz chronionej objętości, w możliwie najkrótszym czasie po detekcji początkowej fazy wybuchu, przez zamontowane czujniki ciśnienia i płomienia. Następuje wówczas natychmiastowe (ok. 20 milisekund) sprowadzenie ciśnienia wybuchu do poziomu zredukowanego i niedopuszczenie do wzrostu ciśnienia powyżej odporności konstrukcyjnej aparatu. Detekcja wczesnej fazy wybuchu odbywa się za pomocą czujników płomienia lub/i ciśnienia. Systemy tłumienia wybuchu są kosztowne, jednak posiadają sporo zalet

In the case of lief systems, there is also the risk of a poorly calculated relief area, failure to take into account the recoil force (foundation of the apparatus), the need to install deflectors, hazards related to the phenomenon, e.g. implosion of tanks.

Flameless venting

Another form of explosion relief is flameless relieving of the explosion. This technique is described in PN-EN 16009:2011 standard. The basic difference between the relief system and a flameless explosion relief system is that the venting effects are free of flame venting, and the temperature of the exhaust gases is reduced. The device, in the simplest terms, consists of a relief mechanism with a mounted flame stopper and heat exchanger. The flame stopper prevents the fire from moving out of the appliance, and the heat exchanger absorbs the high temperature of the exhaust gases. The devices are mainly used indoor, in situations where it is not possible to move the effects of the explosion outside the building. Alas, they have a number of limitations such as: strictly defined requirements as to the size of the room in which they are installed and no installing permit for toxic combustion products. In addition, around devices installed indoor, it is also necessary to determine the so-called safe space, spreading several meters around the device. After mechanism is set off, similarly to an ordinary decompression panel, the system should be disassembled and restored to its full working order by installing the panels under the flameless device. There is also the so-called explosion relief valve, which expands when the explosion occurs, and after the explosion, it self-closes. Such valves can often be found on filters and in dust extraction systems.

Explosion suppression

Another active solution on the market is the active protection system against the effects of an explosion, the so-called HRD (High Rate Discharge Bottles) for explosion suppression. Requirements for this type of system can be found in PN-EN 14373:2006 standard. This system consists of dispersing the suppression agent (suppression powder) inside the protected volume in the shortest possible time after the initial phase of the explosion is detected by the mounted pressure and flame sensors. Then, immediately (within about 20 milliseconds), the pressure of the explosion is reduced to the reduced level and not allowed the pressure to rise above the structural resistance of the appliance. Detection of the early phase of the explosion takes place by means of flame and/or pressure sensors. Explosion suppression systems are expensive, but they have many advantages - the most important ones are the lack of damage to the protected appliance and the lack of fire after the explosion. Systems of this type can be installed for dusts, gases and hybrid mixtures as well as toxic substances. They can be used both indoor and outdoor and cooperate with other systems, e.g. relieving.

W dużym uproszczeniu, zjawisko przeniesienia się wybuchu jest o tyle niebezpiecznym zjawiskiem, że w aparacie, do którego wybuch dotrze z pierwszego urządzenia, zmieniają się całkowicie warunki początkowe, zakładane przy projektowaniu i doborze systemów zabezpieczających.

- do najważniejszych można zaliczyć brak uszkodzeń chronionego aparatu i brak pożaru po wybuchu. Systemy tego typu mogą być instalowane dla pyłów, gazów oraz mieszanin hybrydowych, a także substancji toksycznych. Mogą być stosowane zarówno wewnątrz, jak i na zewnątrz pomieszczeń oraz współpracować z innymi systemami, np. odciążaniem.

Co z przeniesieniem się wybuchu? Odsprzęganie wybuchu

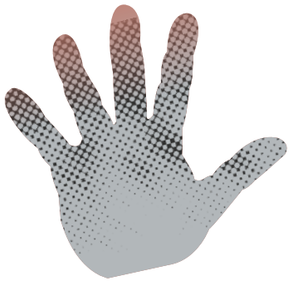
Obniżenie ciśnienia wybuchu poniżej wartości odporności konstrukcyjnej aparatów, realizowane przy pomocy systemów odciążania i tłumienia wybuchu, wymaga w większości przypadków uzupełnienia w postaci systemu izolacji (odsprzęgania) wybuchu (wymagania dla systemu opisane są w normie PN-EN 15089:2010). Odsprzęganie wybuchu jest niestety nierzadko pomijanym systemem ochrony przeciwwybuchowej. W ciągu instalacji procesowych może dojść do zjawiska propagacji wybuchu (fali ciśnienia i płomienia) z jednego aparatu procesowego do kolejnego (pomijając mogące wcześniej wystąpić zjawisko detonacji wewnątrz rurociągu lub kanału).

W dużym uproszczeniu, zjawisko przeniesienia się wybuchu jest o tyle niebezpiecznym zjawiskiem, że w aparacie, do którego wybuch dotrze z pierwszego urządzenia, zmieniają się całkowicie warunki początkowe, zakładane przy projektowaniu i doborze systemów zabezpieczających. Założenia ochrony przeciwwybuchowej dla drugiego aparatu, traktujące go jako oddzielne urządzenie, w przypadku braku systemu odciążenia wybuchu między aparatami będą więc błędne, a cały system ochrony – nieskuteczny. Można zatem powiedzieć, że system odsprzęgania wybuchu jest niezbędnym ogniwem/ składnikiem każdego systemu przeciwwybuchowego, chroniącego dany aparat. Mechanizmy te są również niezbędnym elementem dla urządzeń w wykonaniu odpornym na ciśnienie wybuchu lub tych odpornych na uderzenie ciśnienia wybuchu jako elementy łączące z aparatami w wykonaniu zwykłym. Na rynku dostępne są różne urządzenia: począwszy od systemu HRD (który może również pełnić funkcję izolacji wybuchu), poprzez zasuwy, których zamknięcie wyzwalane jest ładunkiem pirotechnicznym, aż do klap zwrotnych, diverterów, dozowników celkowych, pasywnych

What about the explosion? - Explosion decoupling

Lowering the explosion pressure below the construction resistance value of the devices, implemented with the help of explosion relief and explosion suppression systems, in most cases requires supplementation in the form of an explosion isolation (decoupling) system (requirements for the system are described in PN-EN 15089:2010 standard). Explosion decoupling is unfortunately an often overlooked explosion protection system. In the course of process installations, explosive propagation (pressure and flame wave) can occur from one process device to another (lest mention the possible detonation phenomenon inside the pipeline or duct).

In a matter of fact, the transfer of explosion is dangerous when the explosion reaches from one appliance to another, the initial conditions, assumed in the design and selection of security systems, change completely. If no explosion relief system exists between the appliances, the assumptions of the explosion protection for the other appliance, treating it as a separate device, will be wrong and the whole protection system will be ineffective. It can therefore be said that the explosion decoupling system is an essential link/ component of any explosion-proof system that protects the given appliance. These mechanisms are also a vital element for explosion-proof devices or those with impact-



As a matter of fact, the transfer of explosion is dangerous because in the appliance the explosion reaches from the prior one, the initial conditions, assumed in the design and selection of security systems, change completely.

zaworów dwustronnego działania, zaworów odcinających i śluz ciśnieniowych. Wszystkie te mechanizmy powinny posiadać certyfikat Atex dotyczący możliwości wykorzystania urządzenia jako systemu ochronnego. Należy zaznaczyć, że odpowiedni dobór urządzenia odsprzęgającego (izolującego) wybuch powinien być podparty wnikliwą analizą, począwszy od parametrów zapalności i wybuchowości danego surowca, a skończywszy na wymiarach i geometrii chronionych urządzeń. Dodatkowo dobór urządzeń należy odnieść do warunków i parametrów panujących w instalacji, pamiętając, że każde urządzenie ochronne ma szereg ograniczeń w zastosowaniu, a ich parametry, w zależności od producenta, mogą się różnić.

Serwis – kto i kiedy?

Należy pamiętać, że urządzenia chroniące przed skutkami wybuchu, w myśl polskich przepisów państwowych, zaszeregowane zostały jako urządzenia przeciwpożarowe (§ 2. 1. Punkt 9). Z racji wyżej wymienionego zapisu, urządzenia takie trzeba przeglądać minimum raz w roku. Przepisy państwowe nakładają tylko obowiązek minimalnej częstotliwości przeglądów. Dla każdego z systemów ochronnych – i dla zapewnienia poprawności i utrzymania certyfikatu ATEX dla systemu ochronnego, o częstotliwości wykonywania przeglądów decydują instrukcja obsługi i DTR. W przypadku systemów aktywnych (HRD) i wymagań SIL, przeglądów dokonują akredytowane przez producentów wyspecjalizowane firmy. W przypadku systemów pasywnych, dozowników celkowych, klap zwrotnych, zaworów itp., o sposobie i uprawnionych do przeglądu osobach decyduje dokumentacja producenta.

Podsumowanie

W artykule starano się przybliżyć dostępne na rynku rodzaje systemów zabezpieczenia samych aparatów przed skutkami wybuchu, jak również zasygnalizować niejednokrotnie niedoceniany problem odsprzęgania (odcięcia) wybuchu pomiędzy chronionymi aparatami. Z uwagi na różnice w parametrach substancji stwarzających zagrożenie wybuchowe (Kst i Pmax) oraz w parametrach procesowych, a także dodatkowo biorąc pod uwagę wytrzymałość aparatów i zestawiając z tym ograniczenia w stosowaniu systemów, poprawny dobór systemów ochronnych wymaga indywidualnego podejścia oraz wiedzy i doświadczenia projektanta systemu. ■

resistant explosion pressure as a link to ordinary appliances. There are various devices available on the market: starting from the HRD system (which can also serve as explosion isolation), through gate valves which closure is triggered by a pyrotechnic charge, to the non-return valves, diverters, feeders, passive double-acting valves, shut-off valves and pressure locks. All these mechanisms should have the Atex certificate which allows the use of such device as a protective system. It should be noted that an appropriate selection of an uncoupling explosion device (isolating) should be supported by a thorough analysis, starting from the ignitability and explosive parameters of a given raw material, and ending with the dimensions and geometry of protected devices. In addition, the selection of devices should refer to the conditions and parameters prevailing in the installation, bearing in mind that each protective device has a number of restrictions in application, and their parameters, depending on the manufacturer, may differ.

Service - who and when?

It should be remembered that in accordance with Polish state regulations, devices protecting against the effects of an explosion have been classified as fire-safety devices (§ 2. 1. point 9). Due to this clause, such devices need to be inspected at least once a year. State regulations impose only the obligation of a minimum frequency of inspections. For each of the protective systems, and in order to assure the proper maintenance and to retain the ATEX certificate for the protective system, the frequency of inspections is determined by the instruction manual and the DTR. In the case of active systems (HRD) and SIL requirements, inspections are carried out by specialized companies accredited by producers. In the case of passive systems, cellular feeders, non-return valves, valves, etc., the manufacturer's documentation determines the manner and the persons authorized to make the inspection.

Summary

The article attempts to bring attention to the commercially available types of systems protecting the devices themselves against the effects of an explosion, as well as signaling the undervalued problem of decoupling (cutting off) the explosion between protected appliances. Due to the differences in the parameters of explosive substances (Kst and Pmax) and process parameters, and additionally taking into account the durability of the appliance combined with the limitations in the use of systems, the correct selection of protective systems requires an individual approach and knowledge and experience of the system designer. ■

W SKRÓCIE

• Samego w sobie ryzyka moralnego nie możemy ubezpieczyć, ale już jego skutki tak.

• Fakt posiadania ubezpieczenia powoduje, że ubezpieczony w mniejszym stopniu stara się chronić swoje dobro lub nawet widzi w odszkodowaniu możliwość łatwego zarobku, przez co wzrasta prawdopodobieństwo wystąpienia ryzyka.

IN BRIEF

• We cannot insure moral hazard itslef, but its effects we do.

• The fact of owning an insurance makes the insuree less protective of their property, or even causes them to see the compensation as easy money, which increases risk probability.

Ryzyko moralne / Moral hazard

– czy można je przewidzieć i nad nim zapanować?

Ryzyko moralne, inaczej nazywane pokusą nadużycia (ang. moral hazard), to teza mówiąca o tym, że podmiot chroniony przed ryzykiem może zachowywać się inaczej, niż gdyby był w pełni narażony na ryzyko. Co więcej – posiadacz polisy dostrzega opcję wyłudzenia z niej odszkodowania.

- can it be predicted and controlled?

Moral hazard theory claims that a subject protected against a risk may behave differently than when fully exposed to a risk. What's more - the policy holder recognizes an option of possible compensation extortion.

Krzysztof Dąbrowski

Underwriter, zajmuje się zagadnieniami majątkowymi i technicznymi oraz budowlano-montażowymi, absolwent Wydziału Mechanicznego Politechniki Gdańskiej. W Grupie ERGO Hestia od 2004 r.

Underwriter, dealing with property and technical issues as well as construction and assembly, a graduate of Faculty of Mechanical Engineering at Gdańsk University of Technology. In ERGO Hestia Group since 2004.

Samego w sobie ryzyka moralnego nie możemy ubezpieczyć, ale już jego skutki tak. Wpływ na brak możliwości jego oceny mogą mieć różne czynniki:

a) zmiany trendu na rynku,
b) uzależnienie od jednego dostawcy – odbiorcy,
c) problemy z pracownikami,
d) decyzja władz państwowych.

Zmiany w polityce proekologicznej

Komisja Ochrony Środowiska przy Parlamencie Europejskim przyjęła rezolucję, w ramach której od 2021 roku plastiki jednorazowego użytku (sztućce, talerzyki, kubki, patyczki do uszu) będą zakazane na terytorium Unii Europejskiej.

51 EUROPOSŁÓW GŁOSOWAŁO ZA, 10 BYŁO PRZECIW, A 3 WSTRZYMAŁO SIĘ OD GŁOSU.

Europosłowie chcą także, by odpady z tworzyw sztucznych były poddawane recyklingowi materiałowemu. Powtórne wykorzystanie odpadów z tworzyw sztucznych jest najlepszą metodą usuwania ich ze środowiska. Aktualnie przepisy obowiązujące w Unii Europejskiej zobowiązały Polskę do osiągnięcia min. 50-proc. poziomu odzysku, w tym do 2020 roku 50-proc. poziomu odzysku tworzyw sztucznych z odpadów. Konsekwencją niespełnienia wymagań UE będą wysokie kary finansowe. Z rezolucji wynika też, że do 2025 roku państwa członkowskie będą zmuszone ograniczyć produkty, dla których nie ma alternatywy, tj. m.in. pojemniki na kanapki, owoce, warzywa, desery czy lody. Każde z państw będzie miało też obowiązek stworzenia krajowego planu odpowiadającego za zachęcanie obywateli do używania produktów wielokrotnego użytku oraz takich, które nadają się do recyklingu. Europa odpowiada tylko za niewielką część plastiku zanieczyszczającego nasze oceany, jednak powinna odgrywać kluczową rolę w poszukiwaniu rozwiązań na poziomie globalnym, tak jak to miało miejsce w przeszłości w walce ze zmianami klimatu.

Moral hazard as such cannot be insured, but its consequences can. Various factors may have an impact on the inability to assess it:

a) changes in market trends,
b) dependence on one supplier - recipient,
c) problems with employees,
d) the decision of state authorities.

Changes in the pro-ecological policy

The European Parliament Committee on Environment adopted a resolution under which, from 2021, single-use plastics (cutlery, plates, cups, Q-tips) will be banned within the European Union.

51 MEPS VOTED IN FAVOR, 10 AGAINST AND 3 ABSTAINED FROM VOTING.

EU MEPs also want plastic waste to be recycled. The reuse of plastic waste is the best method of removing it from the environment. Currently, the regulations in force in the European Union oblige Poland to achieve at least a 50% recovery level, including 50% recovery level of plastic by 2020. The consequences of non-compliance with EU requirements will be high fines. The resolution also shows that by 2025 Member States will have to restrict no-alternative products i.e. containers for sandwiches, fruit, vegetables, desserts or ice cream. Each country will also be required to create a national plan to encourage citizens to use reusable and recyclable products. Europe is responsible only for a small part of the plastic polluting our oceans, but it should play a key role in finding solutions on a global level, similarly to its past role in the fight against climate change.

Konieczność zmian

Opisane powyżej zmiany oznaczają powolny koniec bytu zakładów wyspecjalizowanych w produkcji plastikowych jednorazówek. Dodatkowo, jeśli do tego zakład zakupił drogie maszyny do produkcji spersonalizowane na tę działalność, ciężko będzie przekwalifikować się na inną branżę. Co w takim razie zrobić z maszynami, których nikt nie chce kupić a dodatkowo nie nadają się one do przerobienia? Niestety, w takim przypadku może pojawić się plan spieniężenia środków trwałych poprzez odszkodowanie. Polega to na trwałym, jak największym zniszczeniu mienia, aby w zamian otrzymać odszkodowanie. Najczęściej wybieranym sposobem jest podpalenie. W taki sposób można pozbyć się nawet przedmiotów wydawałoby się niepalnych.

Działania długofalowe

Czy istnieje jednak możliwość, aby firmy mogły przekwalifikować się na produkcję z wykorzystaniem wyłącznie materiałów odnawialnych i pochodzących z recyklingu? Należy pamiętać, że przestawienie się na działalność w oparciu o model gospodarki o obiegu zamkniętym nie jest szybkim procesem. Jest to długofalowe i wielowątkowe działanie, które wymaga współpracy między wieloma partnerami, nie tylko komercyjnymi. Zamiana surowców produkcyjnych ze szkodliwych na te bardziej przyjazne środowisku wymaga inwestycji finansowych. Na koszt ten składa się zakup nowych maszyn, przeszkolenie lub nawet zatrudnienie nowych pracowników.

Przykładowo, tworzywa sztuczne z surowca odnawialnego, roślinnego (bioplastik), kosztują obecnie dużo więcej niż konwencjonalne rozwiązania. Produkty takie powinny w przyszłości stać się bardziej powszechne i dzięki temu tańsze. Nie można tutaj jednak zapominać, że nawet najlepsze surowce odnawialne same w sobie nie zlikwidują kwestii jednorazowego użytkowania i odpadów. Ponadto pozostaje jeszcze kwestia przekonania konsumentów do innowacyjnych produktów. Bez zmiany ich przyzwyczajeń i postaw żadna unijna strategia nie będzie miała szansy zadziałać.

Edukacja konsumentów

Obowiązek edukowania konsumentów w kwestii segregacji i recyklingu odpadów spada na państwa unijne oraz na producentów, a nie da się ukryć, że konsumenci są najważniejszym ogniwem tych zmian. Oczywiście można prowadzić różnorodne kampanie połączone z reklamą nowych innowacyjnych produktów, które firma chciałaby wprowadzić na rynek, ale niestety wiąże się to z dodatkowymi, często wielkimi nakładami pieniężnymi.

Necessity of change

The changes described above indicate a slow end to the existence of disposable plastics producers. Moreover, if a plant has purchased expensive dedicated production machines, it will be difficult to reclassify their use to another industry. So what to do with machines that no one wants to take over and that are non-adaptable? Unfortunately, a plan of cashing in on fixed assets through insurance compensation may occur. It means permanent and the greatest possible destruction of such property, in order to receive compensation in return. Arson seems to be the most commonly chosen method so that even seemingly non-flammable objects can be disposed of.

Long-term activities

Still, is it possible that companies could reclassify production using only renewable and recycled materials? It should be remembered that reverting to a circular based economy model is not a speedy process. This is a long-term and multi-threaded operation that requires cooperation between many partners, not only commercial ones. The replacement of production of harmful raw materials to those more environmentally friendly requires financial investments. This cost consists of purchasing new machines, training or even recruitment of new employees.

For example, plastics made of renewable plant-based (bioplastic) raw material currently cost much more than conventional solutions. Such products should become more common in the future and therefore cheaper. However, it should be remembered that even the best renewable resources will not eliminate the one-time use and waste issue. Moreover, the consumers must be first convinced to innovative products. Surely, no EU strategy will work properly unless consumer habits and attitudes are changed.

Consumer education

Educating consumers about segregation and recycling of waste is the responsibility of individual EU member states and producers. Undeniably, it is the consumers who are the key element in the change. Of course, companies may run various campaigns combined with advertising of innovative new products they wish to launch. Unfortunately, it is often associated with additional, often large expenditures.

Ikea, jeden z największych producentów mebli, posiadający także własne restauracje, podejmuje działania, by do 2020 roku wyeliminować plastikowe produkty jednorazowego użytku zarówno z restauracji i bistro, jak i ze sprzedaży we własnych sklepach na całym świecie. Obecnie poszukuje odpowiednich, bardziej ekologicznych alternatyw. I tu pojawia się problem przyspieszonej utraty zbytu produktów, z którą będzie się zmagało wiele firm po znowelizowaniu przepisów dotyczących użytkowania jednorazówek.

Problemy u odbiorcy

Mogłoby się wydawać, że idealnym rozwiązaniem jest kontrakt na sprzedaż własnych wyrobów znanej, wielkiej marce. Wyobraźmy sobie odbiorcę zapewniającego duże obroty i pewny, stabilny zysk. Lecz nagle w krótkim czasie wszystko się zmienia. Decyzją unijną, związaną ze zmianą polityki ekologicznej, odbiorca wyrobów mówi „pas", a cała fabryka zostaje z towarem i brakiem perspektyw zbytu. Jeżeli nie ma planu awaryjnego, staje przed dużym wyzwaniem, co robić dalej.
Nie tylko zaktualizowane przepisy unijne mają wpływ na działalność i współpracę firm. Główny kontrahent może mieć inne problemy powodujące brak możliwości lub chęci wypełnienia kontraktu. Mowa tu choćby o dużej szkodzie wstrzymującej produkcję u samego odbiorcy, powodującej problem ze zbytem, jak również braku ciągłości odbioru wytwarzanego produktu. Przykładem może być wielki pożar z 2015 roku w fabryce General Electric produkującej sprzęt AGD, który spowodował wstrzymanie produkcji na wiele miesięcy oraz zerwanie kontraktów z dostawcami. O ile General Electric mógł się odbudowywać dzięki ochronie ubezpieczenia (majątku, jak również utraty zysku), to już producenci elementów sprzętu AGD, u których szkoda nie wystąpiła, pozostali z towarem i produkcją dedykowaną dla konkretnego odbiorcy.

Zmiana trendu na rynku

Wymagania od dostawców dostosowania się do rynku i zmiany dotychczas wytwarzanych przedmiotów mogą wiązać się z kolejnymi problemami. Po pierwsze, pozostaje nam towar, którego konsument już nie chce, np. nie potrzebuje już płyt CD, zastąpionych przez inne nośniki danych, lub butów, których nie sprzedał w sezonie, a w następnym nie będą już dla klientów atrakcyjne. Niezbędne będą w tym przypadku modernizacje, przeprowadzane również na skutek działań konkurencji, która – wprowadzając nowe rozwiązania i przestawiając się na nowe technologie – optymalizuje swoje procesy produkcyjne i minimalizuje koszty, dzięki czemu może zyskać niebezpieczną przewagę rynkową.

Wprowadzane ulepszenia często są również wymuszane przez zmianę czy też poszerzenie profilu działalności przedsiębiorstwa. Wykorzystywane dotychczas urządzenia mogą w takich sytuacjach okazać się niedostosowane do nowych potrzeb, co z kolei przekłada się na konieczność dużego doinwestowania firmy i powoduje wystąpienie problemów finansowych. Przeinwestowanie często doprowadza do zachwiania stabilności finansowej firmy.

Po drugie, na wpływ finansów rzutuje również kwestia „zapanowania" nad pracownikami. Rosnące z każdym rokiem wynagrodzenia pracowników powodują podwyższenie kosztów wytworzenia produktu. Rynek pracodawcy w obecnym czasie staje się coraz trudniejszy, trudno znaleźć wykwalifikowanych pracowników na linię produkcyjną. Kłopot z siłą roboczą powoduje również, że problemem staje się wyciągnięcie konsekwencji z nadużyć i nieprzestrzegania regulaminu pracy. Natomiast w przypadku, gdy pracodawca zdecyduje się na drastyczne kroki zakończenia współpracy w sposób dyscyplinarny, naraża się na ryzyko moralne ze strony

Ikea, one of the largest furniture manufacturers and restaurant owners, is taking steps to eliminate plastic disposable products from both their restaurants and bistros, as well as from stores sale worldwide by 2020. The company is currently searching for suitable, eco alternatives. Here comes the issue of accelerated loss of products sales, which many companies will struggle with after the regulations on disposables are amended.

Problems with recipients

It might seem that selling own products to well-known, major brand is an ideal solution. Imagine a recipient that ensures high turnover and a stable, assured profit, when suddenly everything changes in in the blink of an eye. Due to EU, pro-ecological decision, the recipient quits and the whole plant is left behind with their stock and no sale perspectives. Without an emergency plan in place, such companies my face a major challenge of what to do next.

Updated EU regulations are not the only factor that has an impact on the operations and cooperation of companies. The main contractor may have other problems resulting in their inability or unwillingness to complete contracts. It could be for instance a major damage resulting in production stoppage at the recipient's, causing a problem with sales, as well as interrupting collection of the manufactured goods.

An example might be the huge fire that took place in 2015 at the General Electric factory producing household appliances. It caused production to stop for many months and the breaking of contracts with suppliers. Thanks to the insurance cover, General Electric was able to recover (property as well as loss of profit), yet manufacturers of some of household appliance components, not affected by the fire directly, were left with stock and production lines dedicated to a specific recipient.

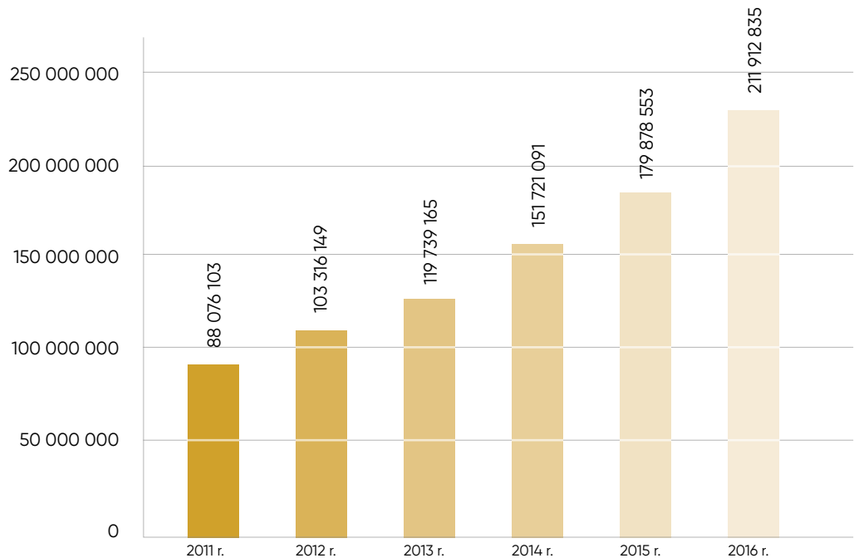
Change in market trends

Some further problems may be associated with the suppliers' requirements to adapt to the market and change previously manufactured items. First of all, there are goods that the consumer no longer wants. For example, consumers no longer need CDs which are replaced by other data carriers - or shoes, which did not sell in the season and thus will no longer be attractive to customers. Hence, the modernizations are vital, also due to market competition, where new solutions and technologies are being introduced, production optimized, costs minimized, and therefore increased competitive advantage gained. Improvements are also often enforced by changing or extending the company's business profile. The devices used so far, may in such situations be unsuitable for the new requirements. It translates into the need for large investment and may create financial problems. Over-investment often leads to financial instability of the company.

The finances may also be affected by the "management" of the employment issue. Remuneration grows year by year, thereby increasing the production costs of the product. Currently, the labor market is becoming increasingly more difficult for the employers, it is hard to find qualified employees for the production lines. The workforce problems also make it difficult to penalize abuse and non-compliance with work regulations. If, however, an employer decides to take drastic steps to terminate the contract in a disciplinary manner, he exposes himself to a moral hazard by the employee. The employee might want to take revenge on the employer and, for example,start the fire at the workplace and in order to settle the score.

WARTOŚĆ PRZESTĘPCZOŚCI UBEZPIECZENIOWEJ W DZIALE II W LATACH 2011-2016 (PLN)

THE VALUE OF INSURANCE CRIMES IN SECTION II 2011-2016 (PLN)



Ogień rozprzestrzeniał się bardzo szybko (...). Straty oszacowano na kilka milionów złotych, a przedsiębiorca pozostał bez możliwości dalszego prowadzenia produkcji i z niewykonanym kontraktem.

pracownika. Oznacza to, że pracownik będzie chciał się odegrać na pracodawcy i w akcie zemsty na przykład podłoży ogień w zakładzie pracy, aby wyrównać rachunki.

Przykładem wyrównywania rachunków może być pożar zakładu stolarskiego z lutego 2014 roku w Kiełpinie. Kamery monitoringu zakładowego nagrały osobę wchodzącą na teren zakładu po jego zamknięciu. Zarzewiem pożaru była znajdująca się na granicy posesji drewniana przybudówka do hali, która zupełnie spłonęła i z której ogień przedostał się na dach głównego obiektu. Sprawca podpalił zapałką folię składowaną w pomieszczeniu przylegającym do stolarni. Mężczyzna w przeprowadzonym postępowaniu przyznał się do winy i usłyszał zarzut sprowadzenia zdarzenia zagrażającego życiu lub zdrowiu. Ogień rozprzestrzeniał się bardzo szybko, zniszczeniu uległa cała hala, w której znajdowały się m.in. meble przygotowane już do transportu. Straty oszacowano na kilka milionów złotych, a przedsiębiorca pozostał bez możliwości dalszego prowadzenia produkcji i z niewykonanym kontraktem.
Kolejnym przykładem jest podpalenie się pracownika w firmie meblarskiej ze stycznia 2018 roku.

46-letni mieszkaniec gminy Bartoszyce z powodu konfliktu z pracodawcą oblał się na terenie zakładu pracy łatwopalną cieczą, a następnie podpalił. Jak podał właściciel zakładu: „ jeden z pracowników zakładu produkcyjnego w Bartoszycach nie został dopuszczony do rozpoczęcia pracy na swojej zmianie z uwagi na niespełnienie warunków BHP”. Konsekwencje takich wydarzeń mogły doprowadzić do ogromnych strat w majątku. Być może zawiodły procedury właściwego usunięcia pracownika z firmy. Tego typu zachowanie jest trudne do przewidzenia i praktycznie niemożliwe do oszacowania na etapie przygotowywania oferty ubezpieczenia.

The fire spread very quickly (...). Losses were estimated at several million PLN, and the entrepreneur ended up without the possibility of further production and with an unfinished contract.

An example of an employee revenge was a fire set to a carpenter's workshop in Kiełpino in February 2014. Factory monitoring cameras recorded a person entering the premises after working hours. The source of the fire was a wooden shed next to the property, which completely burned down and then spread the fire to the roof of the main building. The arsonist set fire to foil stored in the shed. In court, the man pleaded guilty of causing a life- or health-threatening event. The fire spread very quickly and the entire hall was destroyed including furniture already prepared for transport. Losses were estimated at several million PLN, and the owner was left with closed production line and an incomplete contract.

Another example is an employee of a furniture company who set himself on fire in January 2018.
Due to a conflict with his employer, a 46-year-old resident of the Bartoszyce municipality, poured flammable liquid on himself and lit fire to it. The owner of the plant reported then: "one of the employees of the production plant in Bartoszyce was not allowed to start his work shift due to non-compliance with health and safety regulations." It could have led to huge losses in property. Perhaps the procedures failed too. Still, such a reaction of the employees is difficult to predict and practically impossible to estimate while preparing an insurance offer.

Podsumowanie

Według raportu Polskiej Izby Ubezpieczeń (PIU) wyłudzenia stanowią w ogólnej kwocie wypłacanych odszkodowań od 0,28 do 3,70%. Należy pamiętać, że powyższy wskaźnik zależy od skuteczności detekcji przestępstw. Oczywiście statystyki pokazują tylko i wyłącznie przypadki, w których udało się udowodnić próbę wyłudzenia. Część odszkodowań została wypłacona z uwagi na brak możliwości udowodnienia oszustwa. Nie ma możliwości kompletnej oceny ryzyka i wszystkich jego aspektów. Underwriter oceniający ryzyko musi spojrzeć na zagrożenia w większym spektrum – samo opieranie się na informacjach uzyskanych od inżynierów może okazać się niewystarczające. Jak pokazuje życie, nie wszystko da się przewidzieć, ale wiele aspektów, które z pozoru wydaje się bez znaczenia, może mieć diametralny wpływ na losy przedsiębiorstwa i właściwą ocenę ryzyka. Często należy opierać ją nie tylko na konkretnym badanym przedsiębiorstwie, ale również na branży, w której działa, trendach i zagrożeniach makroekonomicznych oraz prawnych, mogących mieć wpływ na prawdopodobieństwo powstania oraz rozmiar szkody. ■

Summary

According to a report by PIU - Polish Chamber of Insurance, extortions constitute 0.28 to 3.70% of total compensations paid. It should be remembered that the above indicator depends on crime detection effectiveness. Of course, the statistics show only proved extort attempts. Some damages were paid due to the lack of evidence of fraud.
It is impossible to complete a full risk assessment and all its aspects. The underwriter must look at the threats in a larger spectrum - the mere reliance on information from the engineers may not be sufficient enough. Life shows not everything, not everything can be predicted but many aspects that are seemingly insignificant can have a huge impact on the business and a proper risk assessment. Often, it should be based not only on a particular company to-be-assessed but also on the whole industry it belongs to, trends, macroeconomic and legal threats that may affect the probability and the size of possible damage. ■

LICZBA, WARTOŚĆ I STRUKTURA PRZESTĘPCZOŚCI UBEZPIECZENIOWEJ WG RODZAJU UBEZPIECZENIA (DZIAŁ II 2016 ROKU)

NUMBER, VALUE AND STRUCTURE OF INSURANCE CRIMES BY TYPE OF INSURANCE (SECTION II 2016)

RODZAJ UBEZPIECZENIA	LICZBA / NUMBER		WARTOŚĆ / VALUE (PLN)		TYPE OF INSURANCE
		(%)		(%)	
OC KOMUNIKACYJNE (MAJĄTKOWE)	5005	52,6%	63 943 333	30,2%	TPL MOTOR INSURANCE
OC KOMUNIKACYJNE (OSOBOWE)	1781	18,7%	23 759 996	11,2%	TPL (PERSONAL)
AUTOCASCO	1893	19,9%	43 752 280	20,6%	MOTOR HULL INSURANCE
OC ROLNIKÓW	63	0,7%	1 872 389	0,9%	LIABILITY OF FARMERS
OD KRADZIEŻY Z WŁAMANIEM (BIZNES)	18	0,2%	671 913	0,3%	BURGLARY (BUSINESS)
OD OGNIA I INNYCH ŻYWIOŁÓW (BIZNES)	28	0,3%	1 804 038	0,9%	FIRE AND OTHER ELEMENTS (BUSINESS)
UBEZPIECZENIA MIESZKAŃ I DOMÓW	171	1,8%	3 478 921	1,6%	INSURANCE OF APARTMENTS AND HOUSES
TURYSTYCZNE I ASSISTANCE	26	0,3%	1 816 918	0,9%	TOURIST AND ASSISTANCE
NNW	246	2,6%	2 094 877	1,0%	ACCIDENT
INNE OC	141	1,5%	2 118 141	1,0%	OTHER LIABILITY
KREDYTY, FINANSE, D&O	7	0,1%	10 587	0,0%	CREDIT, FINANCIAL, D & O
GWARANCJA UBEZPIECZENIOWA	2	0,0%	1 400 492	0,7%	INSURANCE GUARANTEE
INNE*	134	1,4%	65 188 950	30,8%	OTHER*
RAZEM	**9515**	----	**211 912 835**	----	TOTAL

Daniel Świątek

Inżynier ds. Oceny Ryzyka, zajmuje się przeprowadzaniem testów penetracyjnych, audytów teleinformatycznych i szkoleń podnoszących świadomość cyberzagrożeń. Absolwent Wydziału Elektroniki, Telekomunikacji i Informatyki Politechniki Gdańskiej. W Grupie ERGO Hestia od 2017 r.

Risk Assessment Expert, dealing with cyber risk, performing penetration tests, information security audits, and security awareness trainings. A graduate of the faculty of Electronics, Telecommunications and Informatics at Gdańsk University of Technology. In ERGO Hestia Group since 2017.

W SKRÓCIE

- Hakerzy podczas ataku starają się znaleźć słabości w sprzęcie i oprogramowaniu, które umożliwią im przełamanie zabezpieczeń.
- Hakerzy oraz oszuści chcą osiągnąć swój cel przy użyciu jak najmniejszego wysiłku. Zamiast łamać skomplikowane hasła wolą przygotować spersonalizowaną wiadomość phishingową, w której podszyją się pod zaufany serwis i poproszą o podanie do niego hasła.

IN BRIEF

- During an attack, hackers try to find the weak points in the hardware and software that would enable them to break through security systems.
- Hackers and scammers want to achieve their goal with the least effort. Instead of breaking complicated passwords, they prefer to prepare a personalised phishing message in which they act as a trusted service and ask for verification or password.

Socjotechnika wrogiem pracownika / Social engineering – the employee's enemy

W holu pewnej wielkiej korporacji panował ogromny ruch. Pracownicy krzątali się, poszukując w tłumie kontrahentów, osoby ubiegające się o zatrudnienie nerwowo oczekiwały w poczekalni na rozmowę kwalifikacyjną, kurierzy dostarczali przesyłki. Gdyby nie organizacja i chęć niesienia pomocy przez recepcjonistki – z pewnością zapanowałby chaos.

Do recepcji ustawiały się najdłuższe kolejki. Było tak dlatego, że każdy, kto nie był pracownikiem i chciał przejść przez barierki oddzielające część ogólnodostępną od biurowej, musiał pokazać zaproszenie lub uzyskać pozwolenie od kogoś zatrudnionego. Gdy taka zgoda została wydana, recepcja wydawała tymczasowe karty umożliwiające poruszanie się po terenie całej firmy.

(Nie)zawodny system

Cały ten proces przebiegał bardzo sprawnie aż do momentu, w którym wszystkie laptopy w recepcji utraciły dostęp do sieci. Każde wejście musiało być ewidencjonowane w zdalnym systemie, ponadto kontakty do pracowników wyszukiwane były w bazie, do której teraz nie było dostępu. Zgodnie z procedurami, trzeba było przejść na klasyczne metody – zapisywanie wszystkiego w papierowym wykazie gości. Recepcjonistki nie przepadały za tą metodą, bo wiedziały, że później będą musiały wszystko to przepisać do systemu.

In a lobby area of a large corporation and some heavy daily traffic was taking place. Employees busy looking for contractors in the crowd, candidates fidgeting in the waiting room awaiting their interviews and couriers delivering parcels. If not for the well-organised and assistive receptionist, chaos would be inevitable.

The longest queues appeared to be lining up in the reception area. This was because everyone who was not an employee and wanted to go into the office area had to show an invitation or have permit pass from an employee. When such a permission was issued, the person would be given a temporary visitor card that allowed them to move freely around the entire company.

An unreliable system

The entire process seemed to run very smoothly until all the laptops at the reception lost network access. Each entry so far was to be registered in a system. In addition, all the employees contact data was locked in a now unavailable database.. According to the procedures, the receptionist had to revert to the classic method – paper list of the arriving guests. The receptionists were not very fond of this as they knew that later they would have to transfer everything into the system anyway.

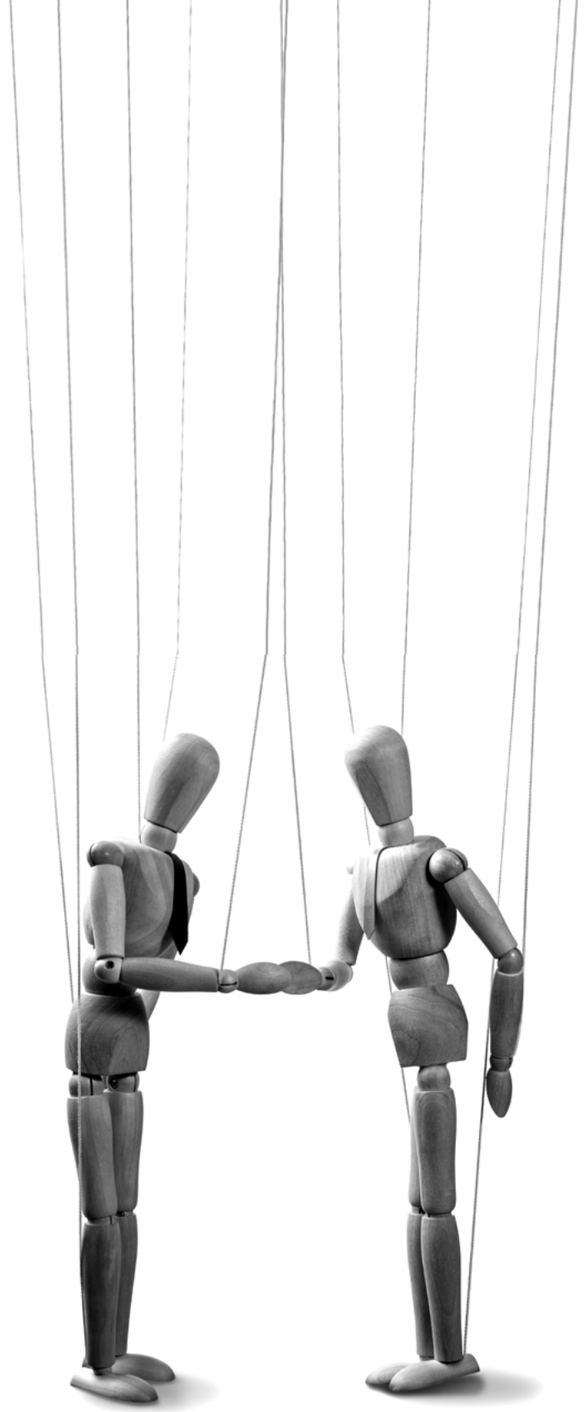
Ludzi ciągle przybywało. Kolejka rosła. Nie było nawet czasu, by zadzwonić do pomocy technicznej. Po około 10 minutach, komputery ponownie połączyły się z siecią, a chwilę później zadzwonił telefon: „Cześć, tu Piotrek z działu IT, widzieliśmy, że miałyście problem z intranetem. Udało nam się go tymczasowo naprawić. Wykryliśmy, że coś było nie tak z jednym z routerów w serwerowni. Jesteśmy tak zawaleni robotą, że nie mamy kiedy dokończyć ich konfiguracji i naprawić tego sprzętu, ale nie martwcie się – zadzwoniliśmy już do serwisu, który to za nas zrobi. Za około godzinę mają przyjechać serwisanci i sprawdzić, co jest nie tak. Pomóżcie nam, proszę, i wpuśćcie ich do środka. Bylibyśmy niezmiernie wdzięczni, gdybyście jeszcze poprosili ochronę o otworzenie im drzwi do serwerowni. Oni już wszystko wiedzą i poradzą sobie sami. My do nich oczywiście później podejdziemy, jak tylko sami odkopiemy się z tych zaległych ticketów".

Fatalna decyzja

Kobieta po chwili namysłu zgodziła się, po czym wróciła do swoich obowiązków. Po około godzinie w holu pojawiły się dwie osoby ubrane w odzież roboczą. W rękach nieśli skrzynki z śrubokrętami, lutownicą i innym sprzętem elektronicznym. „Państwo z serwisu?" – zapytała recepcjonistka i w tym momencie po raz kolejny komputery utraciły połączenie z siecią. „Proszę się tym jak najszybciej zająć, za chwilę ochroniarz pokieruje Państwa do odpowiedniego pomieszczenia". Po około 30 minutach technicy wyszli z serwerowni. Komputery znów działały, więc recepcja z uśmiechem na ustach podziękowała i nie pytając o nic, wypuściła serwisantów. Następnego dnia z nieznanego źródła do internetu wyciekły poufne firmowe informacje. Na domiar złego cała wewnętrzna sieć komputerowa nie działała. Nikt nie znał przyczyn tych incydentów i nie był w stanie powiedzieć, jak do nich doszło.

Hakerskie metody

Hakerzy podczas ataku starają się znaleźć słabości w sprzęcie i oprogramowaniu, które umożliwią im przełamanie zabezpieczeń. Jest to proces bardzo czasochłonny i wymagający sporo wysiłku. Regularna aktualizacja oprogramowania, instalowanie poprawek bezpieczeństwa oraz odpowiednia konfiguracja urządzeń i programów znacząco minimalizuje szansę powodzenia ataku. W takim przypadku wykrycie podatności w systemie jednego dnia nie implikuje jej istnienia w dniu kolejnym. Istnieje jednak jedna słabość każdego systemu teleinformatycznego, która praktycznie zawsze przyczynia się do przełamania zabezpieczeń – jest nią użytkownik. Inżynieria społeczna (zwana również socjotechniką), czyli wykorzystanie w procesie ataku czynnika ludzkiego, jest stosowana przez napastników jako alternatywna droga do przełamania mechanizmów bezpieczeństwa. Przyjrzyjmy się raz jeszcze początkowej historii, przeanalizujmy niekorzystne wydarzenia i prześledźmy całą sytuację z punktu widzenia atakującego.



Inżynieria społeczna (zwana również socjotechniką), czyli wykorzystanie w procesie ataku czynnika ludzkiego, jest stosowana przez napastników jako alternatywna droga do przełamania mechanizmów bezpieczeństwa.

Social engineering, i.e. the use of the human factor in the process of an attack, is used by attackers as an alternative way to break through security mechanisms.

1 NAPASTNICY POCZĄTKOWO WTAPIAJĄ SIĘ W TŁUM – nie jest to trudne w przypadku, gdy dookoła znajduje się pełno ludzi. Osoba siedząca w poczekalni lub kawiarni z laptopem, która jest ubrana zgodnie z panującym w firmie dress code'em, nie wzbudzi podejrzeń, bo w żaden sposób nie odbiega od schematu. Mitem jest przedstawiany przez telewizję obraz hakera jako osoby z kapturem na głowie, siedzącej w kącie z komputerem na kolanach – coś takiego bardzo rzucałoby się w oczy i z pewnością przyciągnęłoby uwagę ochroniarzy lub innych pracowników. Niezwykle trafne w tym przypadku jest powiedzenie, że najciemniej jest zawsze pod latarnią.

2 NASTĘPNYM RUCHEM HAKERÓW JEST ZABLOKOWANIE MOŻLIWOŚCI POŁĄCZENIA LAPTOPÓW Z RECEPCJI Z ROUTEREM WI-FI. Działanie to trwa na tyle długo, aby poirytować recepcjonistki, i jednocześnie na tyle krótko, by nie zostało wykryte przez prawdziwych administratorów. Do wykonania takiej akcji nie potrzeba żadnego wyrafinowanego sprzętu, można to osiągnąć przy użyciu typowego komputera z dokupioną zewnętrzną kartą sieciową, którą podłącza się do portu USB.

3 KOLEJNYM KROKIEM JEST PODSZYCIE SIĘ POD DZIAŁ IT. W przypadku ogromnych korporacji istnieje nikłe prawdopodobieństwo znajomości wszystkich osób z organizacji. Recepcjonistka nie rozpoznaje głosu dzwoniącego, ale jest przekonana, że jest to informatyk – kto inny mógł przecież wiedzieć o tym, że nie działały komputery? „Nie było dostępu do sieci – jest dostęp do sieci, bo informatycy naprawili" – wszystko dla niej w tym momencie składa się w pozornie spójną całość. Haker wykorzystuje teraz tajniki czarnej perswazji, by zmanipulować niczego nieświadomą ofiarę.

4 HAKER W NIEZAUWAŻALNY SPOSÓB GRA NA EMOCJACH KOBIETY, ABY SKŁONIĆ JĄ DO SPEŁNIENIA JEGO PROŚBY. Najpierw napawa optymizmem, informując, że IT wie o zaistniałym problemie i zajęło się nim. Jednocześnie, w tym samym zdaniu, wzbudza niepokój, sugerując, że rozwiązanie problemu jest jedynie tymczasowe, przez co niedogodności i utrudnienia mogą wkrótce pojawić się ponownie. Później wywołuje uczucie litości i współczucia, wspominając o ogromie obowiązków i zadań, które mają

People kept coming. The queue grew longer and longer. There was no time to call for technical support. After about 10 minutes, the computers re-connected to the network, and a moment later the phone rang: "Hi, this is Peter from the IT department, we could see you had some problems with the intranet, but we have fixed it for now. We have detected that something was wrong with one of the routers into the server room. We are so pilled up with work right now that we do not have time to configure them properly and have it up working, but do not worry - we have already called for service and they will do it for us. The service technicians will arrive in about an hour and check what is wrong. Please let them in. We would be extremely grateful if you could also ask the security to let them in to the server room. They already know everything and will manage on their own. We will join them later on, as soon as we have finished the overdue tickets."

A disastrous decision

After a moment of consideration, the woman agreed and then returned to her duties. After about an hour, two workmen appeared in the lobby. They carried boxes with screwdrivers, a soldering iron and other electronic equipment. "Are you the IT service technicians?". At this point, once again, the computers lost the network connection. She said, "Please take care of this as soon as possible, security guard will direct you to the right room." After about 30 minutes, the technicians left the server room. The computers were working again, so the smiling receptionist thanked them and let them go. The next day, some confidential corporate information leaked to the Internet from an unknown source. To make things worse, the entire internal computer network was down. No one knew the cause of these incidents and what really had happened.

Hacker's methods

During an attack, hackers try to find the weak points in the hardware and software that would enable them to break through security systems. It is a very time-consuming process that requires a lot of effort. Regular software updates, installation of security patches and proper configuration of devices and programs significantly minimizes the chance of a successful attack. As such, a vulnerability of the system one day does not imply its occurrence the next day. However, there is one weakness of every IT system that practically always contributes to the break-through - the user. Social engineering, i.e. the use of the human factor in an attack, is used by attackers as an alternative way to break through security mechanisms. Let's review the story once again, analyse the adverse events and review the whole situation from the attacker's point of view.

1 THE ATTACKERS FIRST MINGLED WITH THE CROWD this is not difficult with so many people around. A person sitting in a waiting room or café with a laptop, dressed

do zrobienia. Ostatnie zdanie przed prośbą ma znów pozytywny wydźwięk – jeszcze dziś przyjedzie pomoc i potem wszystko będzie działać jak należy.

5 TERAZ DOCHODZIMY DO KLUCZOWEJ CZĘŚCI ROZMOWY – spowodowanie awarii przez napastników i jej naprawa miały na celu wytworzenie długu wdzięczności, który teraz zostanie wykorzystany. „My pomogliśmy tobie, więc teraz ty pomóż nam" – jest to tak zwana reguła wzajemności. Ludzie przejawiają naturalną chęć do niesienia pomocy i do odwzajemniania się. Odrzucenie tej prośby byłoby dla recepcjonistki niekomfortowe – właśnie przez dług wdzięczności. Wypowiedź napastnika jest bardzo szczegółowa. Używa on pojęć informatycznych takich jak intranet, router, ticket, co jeszcze bardziej utwierdza kobietę w przekonaniu, że jest to Piotrek z działu IT. Kobieta zgadza się na prośbę napastników.

Cel osiągnięty

Pierwszy etap zakończył się sukcesem. Pojawienie się po godzinie w holu osób, które wyraźnie odbiegają od schematu, przykuwa uwagę recepcjonistki. „To muszą być ci serwisanci, o których wspominał specjalista z IT" – zapewne pomyślała kobieta. Tu po raz kolejny napastnicy wykorzystują schematyczność naszego myślenia – jeżeli ktoś ma założoną na siebie sutannę, to od razu zakładamy, że jest to ksiądz, jeśli mundur policyjny – musi to być policjant, a jeśli ubranie robocze, jak w tym przypadku, jest to serwisant. Mamy tu do czynienia z następującym przekonaniem: ubranie odzwierciedla wykonywany przez daną osobę zawód lub status społeczny. Podejrzliwi jesteśmy zazwyczaj jedynie wtedy, gdy nie oczekujemy kogoś lub gdy wykonywałby coś bądź zachowywałby się on niezgodnie z naszymi oczekiwaniami. W momencie, gdy serwisanci zbliżają się do recepcji, dzieje się coś, co po raz kolejny utwierdza kobietę w jej przekonaniu – ponownie zanika połączenie z siecią. Aby jak najbardziej zminimalizować czas trwania usterki, wpuszcza ich ona na teren firmy, zgodnie z wcześniejszą prośbą działu IT i bez jakiegokolwiek sprawdzania tożsamości. Druga część planu również zakończyła się sukcesem – hakerzy, zyskując dostęp fizyczny do sprzętu, omijają wiele zewnętrznych zabezpieczeń, co znacząco usprawnia proces ataku. Mają teraz nienadzorowany dostęp do sprzętu, co wkrótce wykorzystają. Przy ich wyjściu wszystko działa, zrobili swoje. Wychodzą i nikt ich nie sprawdza – ostatnia część planu zakończyła się sukcesem.

Realne zagrożenie

Powyższa historia nie jest wyimaginowana – opiera się na atakach, które miały miejsce w rzeczywistości i są teraz opisywane w podręcznikach do socjotechniki. Pokazuje ona wyraźnie, jak ogromna odpowiedzialność spoczywa na każdym pracowniku. Jego świadomość zagrożeń oraz wiedza dotycząca sposobów uchronienia

according to the company's dress code, will not arouse suspicion as they do not differ from others in any way. The popular TV image of hackers as people with a hood on their heads, sitting in a corner with a computer on their knees is simply a myth –that would be very obvious and certainly attract the attention of security guards or other employees. It is very true to say that the best hiding place is always in plain sight.

2 HACKERS' NEXT MOVE IS TO BLOCK THE POSSIBILITY OF CONNECTING LAPTOPS FROM THE RECEPTION WITH A WI-FI ROUTER.. This action lasts long enough to annoy the receptionists, and at the same time it is short enough not to be detected by the real administrators. No sophisticated equipment is necessary to perform such an action, it can be done using a typical computer with an external network card connected via USB port.

3 THE NEXT STEP IS TO ACT AS THE IT DEPARTMENT WORKERS. In the case of large corporations, there is little chance of personnel knowing all the people in the organization. The receptionist does not recognize the caller's voice but she is convinced that it is one of the company's computer specialists - who else could have known that the computers were not working? „There was no access to the network - then there it is back again because the IT stuff have fixed it" - everything seems so coherent to her then. The hacker now uses the secrets of dark persuasion to manipulate the unsuspecting victim.

4 THE HACKER SECRETLY PLAYS ON WOMAN'S EMOTIONS IN ORDER TO MEET HIS REQUESTS. First, he's optimistic to inform her that IT knows the problem and is working on it. At the same time, in the same sentence, he raises anxiety suggesting that the solution to the problem is only temporary, and that the inconvenience and difficulties may soon reappear. Later, pity and compassion fills the receptionist when hearing of the abundance of responsibilities and tasks the technicians must take care of. The last sentence before the request has a positive tone again - help will come soon and then everything will work as it should.

5 NOW WE COME TO THE KEY PART OF THE CONVERSATION – the hackers, by causing a breakdown and repairing it, aimed at creating a debt

The TV image of hackers as people with a hood on their heads, sitting in a corner with a computer on their knees is a myth – this is something that would be very obvious and certainly attract the attention of security guards or other employees. It is extremely apt in this case to say that the best hiding place is always in plain sight.

Mitem jest przedstawiany przez telewizję obraz hakera jako osoby z kapturem na głowie, siedzącej w kącie z komputerem na kolanach – coś takiego bardzo rzucałoby się w oczy i z pewnością przyciągnęło uwagę ochroniarzy lub innych pracowników. Niezwykle trafne w tym przypadku jest powiedzenie, że najciemniej jest zawsze pod latarnią.

się przed incydentami bezpieczeństwa jest równie ważna, jak wszelkie zabezpieczenia technologiczne, takie jak antywirusy, firewalle, systemy IDS i IPS. Hakerzy oraz oszuści chcą osiągnąć swój cel przy użyciu jak najmniejszego wysiłku. Zamiast łamać skomplikowane hasła wolą przygotować spersonalizowaną wiadomość phishingową, w której podszyją się pod jakiś zaufany serwis i poproszą o podanie do niego hasła.
Pracownicy niewiedzący jak sprawdzić autentyczność odebranej wiadomości i na co zwracać uwagę są niestety bardzo podatni na tego typu zabiegi socjotechniczne. Kliknięcie w zamieszczone w takich wiadomościach linki przenosi użytkowników na kontrolowane przez przestępców wierne kopie zaufanych stron. Podanie

of gratitude that will now be used. „We have helped you, so now you help us" - this is the so-called rule of reciprocation. People are naturally willing to help and to reciprocate. Rejecting this request would be uncomfortable for the receptionist - just because of the debt of gratitude. The attacker is very thorough. He uses IT words such as intranet, router, ticket, which further makes the woman convinced that this is actually the Peter from the IT department. And thus she agrees to the attackers' request.

Target achieved

The first stage was successfully completed. The two persons in working clothes, who appeared in the lobby after an hour, definately caught the receptionist's attention, who supposedly might have thought "these must be the service guys that the IT guy mentioned". Here again, the attackers take advantage of the very schematic nature of our thinking - if someone is wearing a cassock, we immediately assume that it is a priest, if wearing a police uniform - it must be a police officer, and if wearing work clothes, as in this case, it is a service technician. Here comes the common belief: clothing reflects the profession or social status or work performed. We usually get suspicious only if we do not expect someone or if one does something or behaves contrary to our expectations.
When the 'service technicians' approach the reception desk, something that convinces the woman's happens again - the network connection is lost again. To minimize the duration of the breakdown, she allows them to enter the company, as previously requested by the IT department, and what's more, without any identity checks. The second part of the plan was also successful - the hackers gain physical access to the hardware, bypassing many external security devices, which significantly improves the attack process. They now have unattended access to the equipment, which they will soon take advantage of. When they leave, everything seems back to normal, they have done their job. They depart and nobody checks on them - the last part of the plan was a success too.

The real threat

The above story is not imaginary - it is based on actual attacks that have occurred and are now case studies in social engineering textbooks. This clearly shows what great responsibility lies with every employee. The employee's awareness of threats and their knowledge on how to protect the system from security-breach incidents is as important as any technological safeguards, such as anti-viruses, firewalls, IDS and IPS systems. Hackers and scammers want to achieve their goal with the least effort. Instead of breaking complicated passwords, they prefer to prepare a personalised phishing message in which they act as a trusted service and ask for verification or password. Employees who do not know how to verify the authenticity of messages received and do not know what to pay attention to are unfortunately very prone to this type of social engineering. Clicking links in such messages takes users

na nich danych uwierzytelniających jest równoznaczne z przekazaniem ich wprost do rąk przestępców. Administratorzy sieci komputerowych w firmach są świadomi, jak bardzo efektywna jest to metoda, dlatego cała poczta firmowa przechodzi zazwyczaj przez specjalne filtry antyspamowe i antywirusowe. Niestety, zatrzymanie wszystkich takich wiadomości zanim dotrą do użytkowników nie jest możliwe. Mimo bardzo rygorystycznych reguł co jakiś czas przez filtry „prześlizgnie się" niepożądana wiadomość – pokazuje to dobitnie, że świadomość użytkowników musi być dopełnieniem wszystkich mechanizmów bezpieczeństwa, aby działały one sprawnie i efektywnie.

Cyberstatystyki

W przeprowadzonych przez ERGO Hestię badaniach sprawdzana była wiedza i świadomość cyberzagrożeń wśród przedsiębiorców. Poniżej kilka zaczerpniętych z nich statystyk:

- prawie co druga badana firma wskazywała brak świadomości zagrożeń wśród pracowników jako ryzyko dla bezpieczeństwa IT organizacji,
- firmy, które były ofiarami ataków komputerowych, wskazały jako ich przyczynę błędy użytkowników i ich nieświadomość zagrożeń w prawie 40% przypadków,
- aktualni pracownicy byli źródłem ponad 20% incydentów bezpieczeństwa,
- 2/3 wszystkich firm deklaruje, że organizuje szkolenia z bezpieczeństwa dla swoich pracowników.

Nadzieją napawa fakt, że przedsiębiorcy wiedzą o zagrożeniach czyhających na swoich pracowników i organizują dla nich szkolenia podnoszące świadomość. Ważna jest regularność ich odbywania się, tak by nie uśpić czujności użytkowników. Pozostaje jedynie mieć nadzieję, że szkolenia te są czymś więcej aniżeli pokazem slajdów, który użytkownicy przeklikują jak najszybciej i bez zrozumienia. Jak pokazują powyższe punkty, wyeliminowanie lub zminimalizowanie liczby błędów czynnika ludzkiego może zauważalnie zmniejszyć liczbę incydentów. Podnoszenie poziomu wiedzy o cyberzagrożeniach u pracowników jest korzystne dla obu stron: pracodawca zmniejsza ryzyko powodzenia ataku komputerowego na firmę, użytkownik natomiast jest bezpieczniejszy w sieci i nie daje się łatwo oszukać.
Gdyby recepcjonistka z początkowej opowieści zweryfikowała rozmówcę, poinformowała prawdziwy zespół IT o problemach z komputerem i wylegitymowała serwisantów, gdyby wiedziała, jakich technik używają przestępcy, by zmanipulować ofiarę, i zorientowała się, że jest to jedno wielkie oszustwo, wszystko potoczyłoby się zupełnie inaczej, a wyciek informacji byłby wciąż jedynie hipotetyczną sytuacją. ■

to look-alike copies of trusted sites, but controlled by criminals. Providing credentials means transferring all information directly into their hands. Administrators of company computer networks are aware effectiveness this method, which is why the entire company's digital mail usually goes through special anti-spam and anti-virus filters. Unfortunately, it is impossible to stop all such messages before they reach the user. Despite very strict rules, from time to time, unwanted messages will slip through the filters – this clearly shows that the users' awareness must be complementary to all security mechanisms in order to ensure that they work efficiently and effectively.

Cyber statistics

ERGO Hestia have done some research checking the knowledge and awareness of cyber threats among entrepreneurs. Here are some of the outcomes:

- almost every other company surveyed indicated a lack of security awareness among employees as a potential risk to the IT security of the organization,
- companies that have been victims of computer attacks indicated users' errors and employees' unawareness as the cause in almost 40% of the cases,
- current employees were the source of over 20% of security incidents,
- 2/3 of all companies declare that they organize security trainings for their employees.

It is a hopeful sign that the companies are aware of the threads that their employees are exposed to and thus they organize awareness trainings. It is important that they are organised regularly so the users' alertness is not on decline. It can only be hoped that such trainings are something more than only a slide show, quickly clicked through, with no deep understanding. As shown above, eliminating or minimizing the number of human factor errors can noticeably reduce the number of incidents. Increasing knowledge about cyber threats among employees is beneficial for both parties: the employer reduces the risk of a cybernetic attack to the company, while the user is safer using the network and cannot be easily deceived.
If the receptionist in the story had verified the caller, informed the real IT team about the problems with the computer , if she had asked the service people for an ID, if she had been aware of manipulating techniques of the criminals and realized that this was all a big fraud, everything would have turned out differently, and the information leakage would have remained only a hypothetical situation. ■

„Geozagrożenia"

Autorzy: prof. dr hab. Marek Graniczny, Włodzimierz Mizerski
Wydawnictwo Naukowe PWN

Autorzy książki w przejrzysty i rzeczowy sposób opisują największe katastrofy przyrodnicze i ich wpływ na zmieniające się oblicze naszej planety. Prezentowane przykłady pozwalają zrozumieć istniejące w biosferze zależności i wynikające ze zmian niebezpieczeństwa. To drugie wydanie publikacji (pierwsze ukazało się pod tytułem „Katastrofy przyrodnicze"), wzbogacone o aktualne dane i nowy materiał ilustracyjny.

"Geohazards"

Authors: prof. Ph.D. Marek Graniczny, Włodzimierz Mizerski
PWN Scientific Publisher

The authors of the book describe in a clear and factual manner the greatest natural disasters and their impact on the changing face of our planet. The given examples clarify dependencies existing in biosphere and risks that result from changes therein. This is the second edition of the publication (the first one was published under the title "Natural disasters") and it includes current data and new visual material.

VII Międzynarodowa Konferencja HAZEX

BEZPIECZEŃSTWO WYBUCHOWE I PROCESOWE W PRZEMYŚLE

W tym roku – z uwagi na rok nieparzysty – tematyka konferencji zbudowana jest wokół zagrożeń wynikających z obecności w procesie palnych, a tym samym wybuchowych pyłów. Najbliższa konferencja, która odbędzie się w dn. 3-4 października 2019 roku, skupi się zatem na zagadnieniach dotyczących zagrożeń związanych z obecnością w czasie produkcji i magazynowania szkodliwych, palnych i wybuchowych pyłów. Jednym z kluczowych elementów konferencji HAZEX są bowiem demonstracyjne pokazy wybuchów, które pokazują, jakie zagrożenie niosą stosunkowo niewielkie ilości gazów i pyłów powszechnie stosowanych w przemyśle. Zobaczysz wybuchy pyłów na otwartej przestrzeni oraz w zbiorniku zabezpieczonym różnymi technikami (tłumienie wybuchu, odciążanie wybuchu, odsprzęganie wybuchu), a także dostrzeżesz skuteczność oraz zasady działania poszczególnych systemów przeciwwybuchowych.

The 7th International HAZEX Conference

EXPLOSION AND PROCESSING SAFETY MEASURES IN INDUSTRY

This year – being an odd year – the conference is dedicated to risks resulting from processes containing flammable and therefore explosive dusts. The upcoming conference in October 3-4, 2019, will focus on issues related to risks associated with harmful, flammable and explosive dusts appearing during the production and storage stages. One of the key elements of the HAZEX conference is explosion demonstrations. They will illustrate what kind of danger is carried by relatively small amounts of gases and dusts, commonly used in industry. You will see explosions of dust, both in an open space as well as in a closed tank, secured with various techniques (explosion suppression, explosion venting, explosion decoupling) It will demonstrate the effectiveness and operational principles of certain anti-explosion systems.

HESTIA CORPORATE SOLUTIONS

hcs.ergohestia.pl

ERGO HESTIA®

www.ergohestia.pl