

RISKFOCUS

OBLICZA RYZYKA



229 DNI NIEŚWIADOMOŚCI

Pracownik
potrzebny
od zaraz

Dlaczego
maszyny
się psują?

Dym
– wróg publiczny
numer jeden

ERGO
HESTIA®

Realne ubezpieczenie na wirtualny atak #CyberOchrona

- Uszkodzone i zniszczone dane?
- Utrata ciągłości działania?
- Straty wizerunkowe?
- Awaria sprzętu?

Na atak hakerów lub działanie złośliwego oprogramowania narażone jest praktycznie każde przedsiębiorstwo. Czasem nawet najlepsze programy antywirusowe nie są w stanie w porę wykryć zagrożenia.

Cyber ubezpieczenie to pierwszy produkt na naszym rynku, od podstaw przygotowany przez polskiego ubezpieczyciela!

ERGO
HESTIA

Foto na okładce: Dallarphotoclub.com; fot.: STU ERGO Hestia SA

Drodzy
Czytelnicy!



Fala uchoźców przechodząca przez Europę i kryzys Volkswagena – tym żyje świat od kilku tygodni. Zrealizowały się trudne do przewidzenia scenariusze. Mam duże, i chyba uzasadnione, wątpliwości, czy znaleźlibyśmy je w przepowiedniach najsłynniejszego średniowiecznego „menedżera ryzyka” Nostradamusa. Jakże można wyciągnąć z tego wnioski? Po pierwsze, że nic nie jest wieczne, a po drugie, że nie wszystko złote, co się świeci. W tym przypadku złotem jest (czy raczej był) Volkswagen, marka utożsamiana z ponadczasowym designem, bezpieczeństwem i imponującymi osiągnięciami. Teraz stały się one, niestety, prawdziwym przekleństwem. Zobaczmy, jak Volkswagen wybrnie z kłopotów. Koszty będą ogromne, ale może uda mu się wyjść z tego potężnego kryzysu obronną ręką.

Radzenie sobie w trudnych sytuacjach jest coraz częściej tematem rozważań rodzimych przedsiębiorstw. Takie pojęcia jak zarządzanie ryzykiem, ciągłość działania, plany awaryjne nie są już czarną magią, podobnie jak nowe kategorie ryzyka, np. cyber. Ataki hakerów, wirusy komputerowe i inne cyberzagrożenia nie są niczym niezwykłym. Niemal codziennie pojawiają się nowe informacje o skutecznych akcjach „wirtualnych przestępców”. W tym numerze „Risk Focus” znajdzie Państwo artykuł na ten temat. Kontekst ryzyka oraz rozwiązania ubezpieczeniowe powinny Państwu przybliżyć zagrożenia ze strony świata cyber.

Warto też sięgnąć do innych tekstów. Awarie maszyn i urządzeń, systemy oddymiania, bezpieczeństwo flot pojazdów czy pracownicy tymczasowi to tematy, które dla „odkrywców” ryzyka zawsze są interesujące. Kryją się za nimi czysta wiedza i doświadczenie, nie każdy bowiem jest... Nostradamusem.

Zbigniew Żyra

Zbigniew Żyra
Redaktor Naczelny

spis treści
nr 2/2015

RISK CAFE

MAJĄTEK

6 Dym – wróg publiczny numer jeden

12 Dlaczego maszyny się psują?

RYZIKO CYBERNETYCZNE

16 229 dni nieświadomości

**BEZPIECZEŃSTWO
FLOT POJAZDÓW**

24 Szkolenia – lekarstwo dla floty

**ODPOWIEDZIALNOŚĆ
CYWILNA**

30 Pracownik potrzebny od zaraz

NA WŁASNE RYZYKO



Komentujemy teraźniejszy świat ryzyka.
Wejdź na nasz blog: riskfocus.pl

Redaktor Naczelny: Zbigniew Żyra
Koordynacja projektu: Anna Torz
Zespół redakcyjny: Kamil Bara, Hubert Rutkowski,
Jacek Worankiewicz
Druk: Drukarnia WL



Produkcja: Polish Creative Group
(edycja: Bartłomiej Piechocki; layout: Diana Kosiorek;
produkcja: Michał Seredyn; foto: Piotr Bartoszek;
korekta: Elżbieta Woźniak; grafiki: Daria Majchrzak)

Adres: ul. Hestii 1, 81-731 Sopot
tel. (58) 555 62 27
e-mail: risk.focus@ergohestia.pl
www.ergohestia.pl

Z KRAJU



SERYJNE AWARIE turbin wiatrowych

Niedaleko Rymanowa w województwie podkarpackim doszło do awarii elektrowni wiatrowej. Od turbiny odpadł wirnik. W wyniku zdarzenia na szczęście nikt nie ucierpiał.

Elektrownia stoi kilkaset metrów od zabudowań mieszkalnych. Turbinę o mocy 160 kW, wyprodukowaną przez polskiego producenta, oddano do eksploatacji w latach 1999-2000. Jest to jedna z 21 elektrowni pracujących na terenie Rymanowa. To nie pierwsza awaria w tej gminie – wcześniej doszło do oderwania części wirnika elektrowni w Sieniawie, uszkodzenia wirnika innej elektrowni w Rymanowie oraz oderwania wirnika elektrowni pracującej w pobliżu Wróblika Szlacheckiego. ■

NOWE PRAWO budowlane

28 czerwca 2015 r. weszła w życie Ustawa z dnia 20 lutego 2015 r. o zmianie ustawy – Prawo budowlane oraz niektórych innych ustaw (Dz.U. 2015, poz. 443) nowelizująca ustawę z dnia 7 lipca 1994 r. – Prawo budowlane (Dz.U. 2013, poz. 1409, z późn. zm.).

Najistotniejsze zmiany dotyczą zmniejszenia nałożonych na inwestorów obowiązków w kwestii pozwoleń na budowę oraz zgłoszeń budowy do właściwego organu. Jedną ze zmian jest uchylenie przez ustawę obowiązku uzyskiwania pozwoleń na



budowę domów jednorodzinnych, które nie będą uciążliwe dla sąsiadów, np. gdy budynek będzie zbyt blisko ich działki. Zmieniony się niektóre definicje, w tym definicja obiektu budowlanego. Zmodyfikowano także obowiązki uczestników procesu budowlanego oraz niektóre terminy oczekiwania na decyzje administracji. ■

Pokłosie suszy

W sierpniu 2015 r. nad Polskę napłynęła fala afrykańskich upałów. Jej konsekwencją była susza, która dotknęła około 30 proc. polskich gmin.



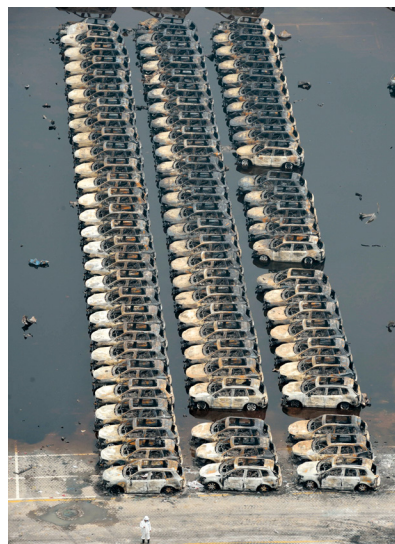
Z opracowania Instytutu Uprawy, Nawożenia i Gleboznawstwa w Puławach wynika, że od 1 lipca do 31 sierpnia zagrożenie suszą wystąpiło wśród upraw roślin strączkowych, ziemniaków, krzewów owocowych, chmielu, kukurydzy na kiszonkę, tytoniu, warzyw gruntowych, buraków cukrowych, drzew owocowych i kukurydzy na ziarno. W skrajnych przypadkach susza spowodowała straty w plonach sięgające 100 proc. Deficyt wody w roku bieżącym był o blisko 270 proc. wyższy niż średnia wieloletnia. Susza utrudniła prawidłowe wykonanie późniejszych zabiegów uprawnych, co spowoduje również straty w przyszłorocznych plonach. ■

ZE ŚWIATA

OGROMNA EKSPLOZJA w chińskim porcie

Zginęły 173 osoby, a aż 797 zostało rannych. To tragiczne skutki serii potężnych wybuchów materiałów niebezpiecznych, do których doszło w sierpniu 2015 r. w jednym z magazynów na terenie portu w Tienlinie w Chinach.

Ustalono, że pierwszy wybuch nastąpił na skutek gaszenia pożaru. Wezwani strażacy, używając wody do gaszenia, wywołali reakcję z acetylenkiem wapnia magazynowanym w miejscu powstania ognia, przez co uwolniono wybuchowy acetylen. Kilkadziesiąt minut później doszło do kolejnych wybuchów, tym razem materiałów wybuchowych i ropy naftowej. Siłę drugiego wybuchu można przyrównać do eksplozji 21 t trotylu. Kulę ognia, jaka powstała, zarejestrował japoński satelita



meteorologiczny. Wybuch spowodował wiele pożarów na pobliskich terenach, czego skutkiem było całkowite zniszczenie sześciu pobliskich budynków oraz uszkodzenie kilku tysięcy nowych samochodów takich marek jak Kia, Hyundai, Volkswagen czy Renault. Kilka dni po zdarzeniu zdecydowano o ewakuacji ludności w promieniu 3 km od miejsca eksplozji, badania ścieków bowiem wykazały 27-krotne przekroczenie normy zawartości cyjanku sodu – silnie trującej substancji. Ustalono, że w miejscu tragedii znajdowało się 700 t tego związku, kilkadziesiąt razy więcej, niż dopuszczają normy składowania. ■

Pechowa budowa LOTNISKA

Kolejny raz przesunięto termin oddania do użytku lotniska Berlin-Brandenburg. Zlecono wymianę 600 nieprawidłowo zbudowanych ścian przeciwpożarowych. Ich konstrukcję wykonano z niewłaściwych materiałów, dlatego należy je zburzyć i wybudować od nowa. Prace mają się zakończyć w marcu 2016 r.



Budowę pechowego lotniska rozpoczęto w 2006 r. Według pierwotnych planów miało być otwarte jesienią 2011 r. Obecnie

mówi się o tym, że lotnisko zacznie działać w drugiej połowie 2017 r. Budowa będzie trwała 10 lat, a jej koszt wyniesie co najmniej 5,4 mld euro, czyli dwukrotnie więcej, niż zakładano w projekcie. Termin otwarcia lotniska przesuwano już czterokrotnie, z powodu licznych usterek technicznych, m.in. niesprawnej instalacji przeciwpożarowej oraz zbyt ciężkich wentylatorów zamontowanych na dachu i zagrożających jego nośności. ■

PRZEMYSŁ



W SPALINACH skandalu

Afera rozpętała się wczesną jesienią tego roku, kiedy Agencja Ochrony Środowiska Stanów Zjednoczonych (EPA) poinformowała, że samochody osobowe z silnikiem 2.0 TDI, wyprodukowane przez koncern Volkswagen AG, wyposażono w oprogramowanie fałszujące dane o emisji substancji szkodliwych. Oprogramowanie wyłączało system neutralizacji tlenków azotu podczas normalnej eksploatacji pojazdu i włączało go w razie rozpoznania, że silnik jest poddawany testom. EPA stwierdziła, że normy emisji tlenków azotu przekraczane były nawet 40-krotnie. VW AG oficjalnie przyznał, że program zainstalowano w 11 mln silników oznaczonych EA 189, w samochodach sprzedanych w USA i Unii Europejskiej. Przedstawiciele niemieckiego producenta chcą przeznaczyć 6,5 mld euro na odbudowę utraconego zaufania klientów. Volkswagen to nie pierwszy koncern oskarżony o oszustwo. W 2014 r. 300 mln dol. zapłaciły Hyundai i Kia, za podawanie nieprawdziwych informacji dotyczących emisji spalin, a w latach 90. podobne problemy miały Ford oraz Honda. Sprawa jeszcze nie została całkowicie wyjaśniona. ■

fot.: Dollarphotoclub.com



WYPADEK w zakładach chemicznych

Podczas prac spawalniczych prowadzonych w zakładach chemicznych w Krupach nad Wełtawą, doszło do wybuchu resztek metanu znajdujących się w zbiorniku.

W wyniku wybuchu obrażenia odnieśli dwaj mężczyźni. Jeden z nich ma poparzoną twarz, drugi uraz ręki. Akcją ratowniczą przeprowadziła zakładowa straż pożarna. Według doniesień policji, przyczyną wybuchu najprawdopodobniej było naruszenie zasad bezpieczeństwa. ■

WYDARZENIA

„WYBUCHY” w Krakowie



Według szacunkowych danych za blisko 60 proc. sytuacji, w których dochodzi do wybuchów pyłów w przemyśle, odpowiadają aparaty i operacje jednostkowe związane z magazynowaniem (silosy), odpylaniem (filtry/cyklony), transportem mechanicznym i mieleniem.

W pozostałych 40 proc. zdarzeń mieszczą się m.in. suszarnie, czynności polerowania i szlifowania, instalacje dopalające, mieszanie oraz przesiewanie. Powyższe dane zostały zaprezentowane podczas III Międzynarodowej Konferencji INDEX – „Bezpieczeństwo wybuchowe i procesowe w przemyśle”, zorganizowanej w dniach 19-20

listopada 2015 r. przez krakowską Grupę Wolff, pod patronatem Ministerstwa Gospodarki. Ze względu na powtarzające się zdarzenia niebezpieczne z udziałem pyłów wybuchowych zagadnienia prewencji, aktualnych wymogów prawnych oraz technicznych rozwiązań służących ograniczeniu skutków wybuchów, powinny w najbliższych latach stanowić przedmiot wzmożonego zainteresowania osób zajmujących się szeroko rozumianą prewencją oraz bezpieczeństwem w przemyśle. ■

CYBER

HA(TA)CK na Dow Jones



Trwa śledztwo w sprawie ataku hakerskiego na Dow Jones, do którego doszło 16 października. Głównym zadaniem FBI jest oczywiście precyzyjne określenie, kto za nim stoi.

Zastanawiające jest, czy to ciąg dalszy cyberwojny, czy może „niewinne” cyberspiegostwo. Niezależnie od powodów, amerykańskie cyberusługi mogą się wykazać, wykrywając sprawcę ataku.

Włamanie od strony infrastruktury teleinformatycznej Dow Jones zostało poprzedzone kilka dni wcześniej innym atakiem, który mógł mieć charakter preludium. Częstym zjawiskiem w procesie kompromitacji systemu jest wcześniejsze rozpoznanie zabezpieczeń poprzez umiejętne skanowanie infrastruktury ofiary, aby zwiększyć skuteczność właściwego ataku.

W obliczu wydarzeń z feralnego piątku, prorocze wydają się słowa prezydenta Baracka Obamy, które wypowiedział po podpisaniu porozumienia z Xi Jinpingem, w sprawie zaprzestania wspierania cyberkradzieży własności intelektualnej: „This is progress, but (...) our work is not yet done”. ■

DYM

– wróg publiczny numer jeden

ZRYWASZ SIĘ W ŚRODKU NOCY Z HOTELOWEGO ŁÓŻKA OBUDZONY GŁOŚNYM SYGNAŁEM ALARMU POŻAROWEGO. PEŁEN OBAW OTWIERASZ DRZWI I WYCHODZISZ NA SPOWITY DYMEM KORYTARZ. W GŁOWIE MASZ TYLKO JEDNĄ MYŚL: JAK DOTRZEĆ DO WYJŚCIA EWAKUACYJNEGO?

Tekst: Mateusz Kiliszek

W idząc kłęby dymu, możemy przypuszczać, że jest on efektem pożaru. Wiele osób traktuje go wyłącznie jako oznakę pożaru. To błąd. Produkty spalania mają właściwości toksyczne i stanowią realne zagrożenie dla życia i zdrowia człowieka. Są także szkodliwe dla mienia.

CZYM JEST DYM?

Skład dymu zależy od wielu czynników. W głównej mierze od rodzaju spalanego paliwa oraz warunków spalania. Dokładne określenie składu dymu jest trudne, a często wręcz niemożliwe, np. podczas rozkładu termicznego drewna wydzielają się ponad 200 związków o właściwościach toksycznych. W praktyce podczas oceny szkodliwości środowiska pożarowego przeprowadzana jest analiza wyłącznie produktów rozkładu głównie ponoszących winę za wypadki śmiertelne (CO , CO_2 , HCl , HCN , SO_x , NO_x , HBr).

Co do zasady pożar, podczas którego występuje niedobór powietrza, charakteryzuje się większą ilością substancji szkodliwych w produktach spalania. Dym powstały podczas takiego spalania będzie miał ciemną barwę, co wynika z obecności w nim cząsteczek węgla.

DYMNE ZAGROŻENIA

W literaturze przedmiotu najczęściej rozważa się zagrożenia, jakie dym stwarza dla życia i zdrowia ludzi. Znacznie rzadziej rozpatruje się ten temat w kontekście ochrony mienia. Tymczasem rozprzestrzeniający się w obiekcie dym, stykając się z różnymi przedmiotami, powoduje ich zanieczyszczenia. Ich intensywność i obecność zależą od:

- liczby i rodzaju elementów objętych pożarem,
- przebiegu pożaru,
- sposobu odprowadzania dymu.

Część zanieczyszczeń można łatwo usunąć, jednak w określonych przypadkach okazuje się to trudne, a czasem nawet niemożliwe. Dodatkowo niektóre produkty spalania mogą powodować korozję. Dobrym przykładem jest polichlorek winylu, który ze względu na właściwości jest najczęściej stosowanym tworzywem w budownictwie. Na świecie zużywa się go około 26 mln t rocznie. Tworzywo to występuje w wykładzinach, urządzeniach elektronicznych, elektronice przemysłowej, lakierach, materiałach biurowych.

Jednym z produktów spalania polichloru winylu jest chlorowodór, który pod wpływem wilgoci może się przekształcić w kwas solny. Ze spalania 1 kg PCV, w określonych warunkach, może

powstać więcej niż 1 kg kwasu solnego. Substancja ta może zainicjować procesy korozyjne stali (również ocynkowanej), cyny, miedzi i aluminium. Narażone na jej działanie powłoki lakiernicze mogą się odbarwiać lub zmieniać. Jednak największe zagrożenie kwas solny stano-

DYM

to wydzielany aerozol, którego głównym źródłem są procesy spalania (PN-ISO 4225:1999).

wi dla urządzeń elektronicznych, które pod jego wpływem mogą zniszczyć się w sposób nieodwracalny.

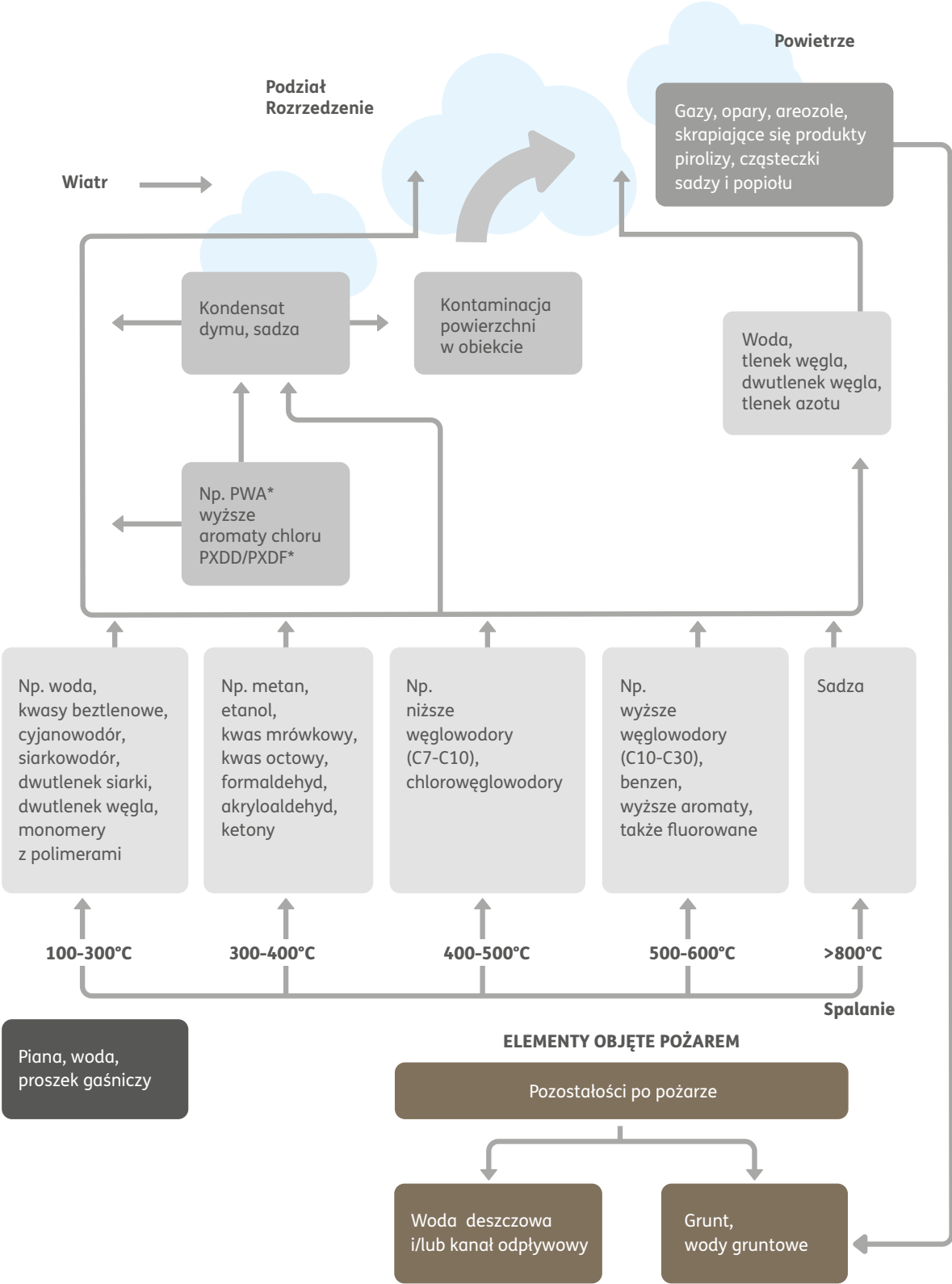
Rozmiar szkody spowodowanej zadymieniem nie zawsze wynika bezpośrednio ze skali pożaru. Klasycznym scenariuszem takiego przypadku jest pożar śmietnika w magazynie hurtowni farmaceutycznej. Rozmiar szkody spowodowany bezpośrednim oddziaływaniem ognia byłby marginalny. Natomiast uszkodzenia spowodowane oddziaływaniem dymu, mogą spowodować konieczność utylizacji większości środków obrotowych zgromadzonych w magazynie. Konieczność utylizacji wynika z wymagań odpowiednich przepisów prawa oraz instytucji nadzorujących.

OCZYŚCIĆ ATMOSFERĘ

Skutki działania dymu oraz gazów pożarowych można znacznie ograniczyć poprzez stosowanie wentylacji pożarowej. Wykorzystanie tego typu systemów w niektórych obiektach, stanowi podstawę do spełnienia wymagań zawartych w Rozporządzeniu Ministra Infrastruktury z 12 kwietnia 2002 r. (Dz.U. nr 75, poz. 690) w sprawie warunków technicznych, jakim powinny odpowiadać budynki i ich usytuowanie. Ponadto zastosowanie systemu oddymiającego pozwala powiększyć dopuszczalną strefę pożarową, a także wydłużyć przejścia i dojścia ewakuacyjne. Można więc wnioskować, że systemy tego typu pełnią ważną rolę w ochronie przeciwpożarowej. Dlatego też ich niezawodność powinna zostać utrzymana na najwyższym poziomie.

Temat wentylacji pożarowej jest bardzo rozległy. Mnogość systemów, urządzeń oraz sposoby ich wykorzystania, generują problemy projektowe, wykonawcze oraz





Podział systemów wentylacji pożarowej

Cel	Wentylacja oddymiająca	Kontrola dymu i ciepła	Oczyszczanie z dymu	Zabezpieczenia dróg ewakuacji
Rodzaj	Wentylacja grawitacyjna	Wentylacja strumieniowa	Wentylacja mechaniczna	Zabezpieczenie przed zadymieniem – systemy grawitacyjne
	Wentylacja mechaniczna	Systemy cross ventilation	Wentylacja grawitacyjna	Zabezpieczenie przed zadymieniem – systemy mechaniczne
			Systemy cross ventilation	Zabezpieczenie przed zadymieniem – systemy mieszane
				Zabezpieczenie przed zadymieniem – systemy nadciśnieniowe

eksploatacyjne. Ponadto, projektując system wentylacji pożarowej, należy zapewnić jego współpracę z innymi instalacjami służącymi bezpieczeństwu pożarowemu w obiekcie. Sytuacja tego typu bardzo często spotykana jest w obiektach produkcyjno-magazynowych, w których zainstalowano klapy oddymiające oraz stałe urządzenia gaśnicze tryskaczowe. Zbyt wczesne zadziałanie systemu oddymiania opóźni zadziałanie urządzenia gaśniczego. W takiej sytuacji rozmiar potencjalnej szkody może znacząco się powiększyć. Znane są również przypadki szkód, w których wentylacja pożarowa uniemożliwiła zadziałanie instalacji gaśniczych, powodując całkowite zniszczenie obiektu. Z drugiej strony zbyt późne zadziałanie wentylacji może utrudnić przeprowadzenie ewakuacji w określonych warunkach, np. wówczas, gdy dym i gazy pożarowe nie zostaną odprowadzone z drogi ewakuacyjnej. Wyzwolone stałe urządzenie gaśnicze tryskaczowe spowoduje przechłodzenie dymu i jego opadnięcie. W takiej sytuacji wymóg wolnej przestrzeni od dymu może zostać niezachowany.

Prawidłowa eksploatacja systemów wentylacji pożarowej wymaga dokonywania regularnych przeglądów. Ale praktyka pokazuje, że nie zawsze wszystkie elementy instalacji są sprawdzane. Przykładem mogą być naboje gazowe zawierające sprężony dwutlenek węgla, zapewniający energię do otwarcia klapy oddymiającej. Podczas przeglądów często pomijane jest sprawdzanie gazu, który w nich pozostaje. Jeśli naboje gazowe będą go

miały zbyt mało, klapy oddymiające mogą nie zadziałać prawidłowo.

Jedną z możliwych klasyfikacji systemów wentylacji pożarowej jest rozróżnienie ich ze względu na cel oraz rodzaj zastosowanych urządzeń.

WENTYLACJE ODDYMIAJĄCE
Głównym celem stawianym przed instalacjami oddymiającymi jest utrzymanie wolnej od dymu przestrzeni, tak aby były zachowane odpowiednie warunki do ewakuacji, a stopień kontaminacji mienia przez produkty spalania był jak najniższy. Ponadto wentylacja oddymiająca odprowadza gorące gazy pożarowe (o temperaturze do 1000°C), chroniąc w ten sposób konstrukcję budynku przed uszkodzeniami. >>

WENTYLACJA POŻAROWA

– systemy i urządzenia mające na celu ograniczenie skutków pożaru poprzez usuwanie i kontrolę powstającego dymu oraz gazów pożarowych.



Oddymianie może odbywać się zarówno w pomieszczeniu zagrożonym, jak i poprzez obszar wspólny dla większej liczby małych pomieszczeń, np. w pasażach handlowych. Wentylację tego typu możemy najczęściej spotkać w:

- jednokondygnacyjnych budynkach wielkopowierzchniowych (produkcyjnych, magazynowych, usługowych),
- garażach,
- drogach ewakuacji,
- pasażach handlowych.

Wentylacja oddymiająca może być realizowana za pomocą systemu grawitacyjnego lub mechanicznego. System grawitacyjny najczęściej składa się z klap oddymiających i napowietrzających. Zaznaczyć tu należy, że w zależności od obiektu, stosowane są nie tylko kłapy, ale również inne rozwiązania, takie jak: okna fasadowe, świetliki, żaluzje itp. Pracą tych elementów zarządza odpowiedni system, który w przypadku pożaru automatycznie oraz w odpowiedniej sekwencji otwiera elementy oddymiające i napowietrzające. Niektóre systemy wyposażone są w funkcję przewietrzania. Użytkownik systemu w takim przypadku może ręcznie otworzyć kłapy. Nowoczesne centrale sterujące wyposażone są również w czujniki pogodowe. Umożliwiają one prowadzenie kontrolowanej wentylacji pomieszczeń przy minimalizacji ryzyka uszkodzenia klap w wyniku działania wiatru oraz ryzyka zalania budynku spowodowanego opadami atmosferycznymi.

Pamiętać należy, że aby system takiego typu był skuteczny, różnica temperatury pomiędzy otaczającym powietrzem a dymem musi być większa niż 100°C. Jeżeli różnica temperatur jest niższa, sprawność systemu może być ograniczona. Omawiane rozwiązanie nie może być stosowane dla pomieszczeń o powierzchni poniżej 600 m², o ile ich wysokość nie przekracza 6 m.

Jeżeli zastosowanie oddymiania grawitacyjnego jest niemożliwe, stosuje się systemy mechaniczne. Zdarza się to najczęściej w budynkach wielopiętrowych, pomieszczeniach piwnicznych lub pomieszczeniach położonych w środkowej części budynku. Tego typu systemy oprócz funkcji wymuszonego usuwania dymu i gazów pożarowych, pełnią również rolę standardowej wentylacji. Wentylatory mogą być montowane pod dachem, w ścianie lub w kanałach wentylacyjnych. Najczęściej stosowane rodzaje wentylatorów:

- dachowe,
- osiowe,
- kanałowe,
- strumieniowe.

Podobnie jak w przypadku wentylacji grawitacyjnej, do prawidłowego działania wymagane jest zapewnienie odpowiedniego systemu napowietrzania. Wentylatory powinny mieć przynajmniej dwa niezależne i pewne źródła zasilania.

KONTROLA DYMU I CIEPŁA

Systemy tego rodzaju znajdują zastosowanie w garażach, dokach dostawczych i przejazdach w garażach zamkniętych. Pełnią one również funkcję wspomagającą działanie ekip ratowniczo-gaśniczych. System wentylacji tego rodzaju działa dwuetapowo. Pierwszym etapem jest ewakuacja, podczas której wentylatory nie powinny pracować. Po zakończeniu ewakuacji, całość systemu może zostać uruchomiona.

Głównym zadaniem stawianym tego rodzaju systemom jest ograniczenie rozprzestrzeniania się ciepła i dymu, pomiędzy miejscem zdarzenia pożarowego a punktem ich usunięcia. Wentylacja spełniająca ten warunek, umożliwia podjęcie skutecznej akcji gaśniczej oraz ogranicza rozmiar szkód.

Zaprojektowanie systemu kontroli dymu i ciepła wymaga opracowania odpowiedniego jego działania. Kierunek wentylacji powinien gwarantować jak najkrótszą drogę do szachtu wywiewnego wentylacji. Ważne jest również, aby same szachty miały odpowiednią wydajność. Znane są przypadki ich niedowymiarowania.

OCZYSZCZENIE Z DYMU

Celem systemów oczyszczania z dymu jest ograniczenie ilości dymu i gazów pożarowych do takiej, która nie stwarza zagrożenia dla znajdujących się w strefie ludzi. Ten rodzaj wentylacji jest z założenia najmniej efektywny (dopuszcza obecność dymu) i nie powinien być stosowany jako zamiennik wymaganych przepisami prawa systemów. Oczyszczanie z dymu można zrealizować za pomocą wentylacji przewodowej oraz wentylacji strumieniowej.

ZABEZPIECZENIE DRÓG EWAKUACJI

Bezpieczeństwo dróg ewakuacji można zapewnić na dwa sposoby. Pierwszym z nich jest zabezpieczenie przed zadymieniem, takie że dym z dróg ewakuacyjnych odprowadzany jest poprzez system wentylacji oddymiającej (mechaniczna, grawitacyjna lub mieszana). Drzwi do chronionych obszarów powinny zostać wyposażone w samozamykacze.

Drugim wariantem zabezpieczenia dróg ewakuacyjnych jest zapobieganie zadymieniu. Działanie tego typu

systemów polega na nawiewie świeżego powietrza do chronionych stref przy jednoczesnym zapewnieniu jego upustu w miejscu wystąpienia pożaru. Tak jak w przypadku zabezpieczenia przed zadymieniem, drzwi chronionych obszarów należy wyposażyć w samozamykacze.

Wysterowanie tego typu systemów jest niezwykle trudne. Do regulacji systemu wykorzystywane są: kłapy transferowe, kłapy upustowe, regulatory wydajności wentylatorów. Nieprawidłowoysterowany system może wytworzyć zbyt wysokie ciśnienie na klatce schodowej, przez co przeprowadzenie ewakuacji staje się niemożliwe. Przy działającym systemie siła potrzebna do otworzenia drzwi nie powinna przekroczyć 100 N.

Systemy wentylacji pożarowej nie są w stanie całkowicie zabezpieczyć obiektów przed skutkami działania gazów pożarowych oraz dymu. Umożliwiają jednak ewakuację, a w określonych okolicznościach ograniczają rozmiary szkód. Funkcję tę jest dość trudno osiągnąć z powodu złożoności dostępnych na rynku systemów oraz konieczności ich integracji z innymi zainstalowanymi w budynku urządzeniami służącymi bezpieczeństwu pożarowemu.



Mateusz Kiliszek

Absolwent Wydziału Inżynierii Łądowej i Środowiska oraz Wydziału Zarządzania i Ekonomii na Politechnice Gdańskiej, absolwent Coventry University – European Engineering Business Management. W Grupie ERGO Hestia od 2013 r.



mateusz.kiliszek@ergohestia.pl



DLACZEGO maszyny się psują?

WYNALEZIENIE SILNIKA PAROWEGO PRZEZ JAMESA WATTA I OPATENTOWANIE GO W ANGLII W 1769 R. DAŁO POCZĄTEK UPRZEMYSŁOWIENIU NA DUŻĄ SKALĘ. NA POCZĄTKU XIX W. PRODUKCJA I WYKORZYSTANIE MASZYN RUSZYŁY PEŁNĄ PARĄ. W TAMTYM CZASIE CECHOWAŁY SIĘ ONE WYSOKĄ AWARYJNOŚCIĄ – ZE WZGLĘDU NA NISKI POZIOM WIEDZY TECHNICZNEJ, STOSOWANE TECHNOLOGIE WYTWARZANIA ORAZ MAŁO SKUTECZNE ZABEZPIECZENIA. A DZISIAJ? MOŻNA BY OCZEKIWAĆ, ŻE PO DWÓCH WIEKACH DYNAMICZNEGO ROZWOJU NAUKI I WSZYSTKICH DZIEDZIN TECHNIKI MASZYNY NIE BĘDĄ SIĘ PSUŁY. JEDNAK TAK NIE JEST.

Tekst: Ryszard Boyke

NIE MA MASZYN DOSKONAŁYCH

Czas życia maszyny należy liczyć od pierwszych założeń techniczno-ekonomicznych, obejmuje on potem projektowanie, budowę, montaż, rozruch, okres użytkowania, wreszcie wycofanie maszyny z eksploatacji. Urządzenia nie powinny być, i zazwyczaj nie są, eksploatowane do – mówiąc potocznie – „zajechania”, czyli stanu, w którym nie nadają się już do naprawy. Ich wycofanie z eksploatacji następuje najczęściej z przyczyn ekonomicznych, gdy maszyna po przeprowadzeniu standardowego przeglądu i naprawy, nie osiąga swoich nominalnych parametrów, lub jeżeli jej wydajność i jakość wytwarzanych produktów, przestają być akceptowalne na rynku, przy uwzględnieniu konkurencyjnych cen.

Przyczyny awarii mogą się wiązać z każdym etapem budowy i aspektem użytkowania maszyny. Z moich doświadczeń – jako inżyniera zajmującego się oceną ryzyka ubezpieczeniowego maszyn i urządzeń – wynika, że w procesach produkcyjnych o małej złożoności, przyczyną awarii częściej są błędy wykonawcze i montażowe. Natomiast przy stosowaniu skomplikowanych technologii awarie znacznie częściej są skutkiem błędów eksploatacyjnych.

OD PROJEKTU DO BUDOWY

Można przyjąć, że błędy w dokumentacji projektowej, wynikające z pomyłek w obliczeniach, występują rzadko. Częściej spotykamy się z doбором niewłaściwych materiałów lub nieprawidłowym wykonaniem głównych podzespołów maszyny. Pomimo kontroli jakości prowadzonej przez producenta, i to z użyciem specjalistycznych urządzeń, nie udaje się wychwycić wszystkich usterek. Błędy, które nie zostały wykryte, z całą pewnością w przyszłości doprowadzą do awarii. Wydaje się, że jedną z przyczyn tego stanu są wymagania rynku, który oczekuje od producentów – i w jakimś stopniu wymusza to na nich – budowy coraz bardziej wydajnych maszyn, jednocześnie tańszych przy zakupie i w przyszłej eksploatacji. To musi prowadzić do większej podatności urządzeń na awarie.

MONTAŻ NA STANOWISKU I ROZRUCH

Błędy podczas montażu maszyny na stanowisku nie zdarzają się często. Miejsce jej ustawienia jest sprawdzane, a wszystkie zauważone usterki i niedociągnięcia zostają usunięte. Pomijam zagrożenia występujące podczas przeładunków i transportu urządzeń. Odbywa się to z zachowaniem wymagań producenta oraz

ogólnych zasad bezpieczeństwa. Nie jest dobrze, jeśli realizacja inwestycji się opóźnia, ponieważ urządzenia dostarczane są na budowę w terminach zgodnych z zamówieniem. Dochodzi do takich sytuacji, że budynki produkcyjne, w których miały być zainstalowane urządzenia, nie są jeszcze do tego przygotowane.

Przywiezione maszyny należy przechować, jednak nie ma gdzie, ponieważ pierwotny harmonogram budowy zakładał dostawę bezpośrednio na stanowisko montażu. Potrzebny jest magazyn, szczególnie jeśli urządzenia nie mogą być składowane na placu, bo są np. wrażliwe na pył. Niektóre wręcz wymagają pomieszczeń magazynowych z klimatyzacją. Budowa magazynu w takim przypadku odpada z dwóch powodów. Po pierwsze wymaga czasu, a po drugie podnosi koszty inwestycji, na co inwestorzy nie patrzą przychylnym okiem. Stawiane są więc na prędko hale namiotowe, wynajmowane budynki, które przystosowuje się do funkcji magazynu. Jednym słowem – improvisacja. Próby dodatkowego zabezpieczenia urządzeń i opracowane w przyspieszonym tempie sposoby konserwacji nie zawsze są do zaakceptowania przez ubezpieczycieli. Bywa, że urządzenia >>



Naprawa uszkodzonej maszyny czy zakup nowej, to nie wszystkie koszty, które trzeba ponieść.

Awaria maszyny może zagrażać zdrowiu, a nawet życiu operatora. Spowoduje zatrzymanie linii produkcyjnej i, co za tym idzie, doprowadzi do niewywiązania się z umowy handlowej na dostawę wyrobów.

w nieodpowiednich warunkach leżakują nawet do kilkunastu miesięcy. W efekcie, po przekazaniu maszyn do eksploatacji, ryzyko ich awarii wzrasta. Zdarzały się przypadki cofnięcia przez producenta gwarancji na bezawaryjną pracę maszyny. Montaż maszyn na stanowisku nie powoduje zwiększenia ryzyka awarii w przyszłej eksploatacji – zajmują się tym przedsiębiorstwa ze znajomością branży, zatrudniające ludzi o wysokich kwalifikacjach, którzy swoje doświadczenie zdobywali i pogłębiali na niejednej budowie. Urządzenia o wysokim stopniu złożoności, gdy

wymaga tego technologia, montowane są pod nadzorem specjalistów producenta.

Po zakończeniu montażu przeprowadza się próby pomontażowe, nazywane często „rozruchem zimnym”. Wszystko odbywa się pod kontrolą inspektorów nadzoru. Na tym etapie ryzyko popełnienia błędu, który w przyszłości mógłby skutkować awarią, jest niewielkie. Prawdopodobieństwo uszkodzenia maszyny wzrasta podczas rozruchu technologicznego, czyli pierwszej próby rozpoczęcia produkcji. Do instalacji podawane są media, podejmuje się próby osiągnięcia znamionowych parametrów procesu, niekiedy tych najbardziej niebezpiecznych, tj. temperatur, ciśnienia lub próżni, prędkości obrotowych elementów wirujących. Sprawdza się działanie układów sterowania, sygnalizacji, blokad technologicznych i zabezpieczeń. Jest to czas na regulację aparatów i korektę nastaw zabezpieczeń. Oprócz nadzoru inwestorskiego w rozruchu technologicznym biorą udział specjaliści ze strony producenta lub autoryzowanych firm serwisowych. Po jego zakończeniu wykonuje się jeszcze próby dochodzenia do tzw. parametrów gwarantowanych, czyli przyjętej w dokumentacji i oczekiwanej przez inwestora

wydajności, sprawności itp. zarówno poszczególnych urządzeń, jak i całej linii technologicznej. Praktyka pokazuje, że może to trwać od kilku do nawet kilkunastu tygodni. Dobrze, jeśli popełnione wcześniej błędy w projektowaniu, doborze materiałów czy podczas budowy maszyny, zostaną wykryte na etapie testów i prób. Nawet gdyby doszło do awarii, to koszty jej usunięcia będą mniejsze niż podczas eksploatacji. Na miejscu są przecież ekipy montażowe, łatwiej o części zamienne i materiały eksploatacyjne. Nie bez znaczenia jest to, że w takim przypadku koszty remontu prawie zawsze ponosi dostawca maszyny. Strata inwestora wynika wówczas jedynie z opóźnienia terminu zakończenia inwestycji i braku przychodów z planowanej sprzedaży.

I WRESZCIE EKSPLOATACJA

Pomijam wpływ czynników atmosferycznych, takich jak: deszcz, śnieg, mróz, wysoka temperatura w miejscach nasłonecznionych. Pomijam zagrożenia procesowe wynikające z technologii, a także działanie szkodliwych czynników zewnętrznych w budynkach, np. wilgoci, związków chemicznych itp. Pomijam również ryzyko procesowe. Zakładam, że maszyna jest konstrukcyjnie dostosowana do warunków, w których ma pracować, i funkcji, jakie ma pełnić.

Nie bez znaczenia dla odporności maszyny na uszkodzenia jest liczba przepracowanych godzin, uruchomień i wyłączeń oraz stanów szczególnych, gdy przekraczane są znamionowe parametry pracy. Na szczęście, czas eksploatacji to również okres, gdy podejmowane są czynności, których celem jest ograniczenie ryzyka uszkodzenia maszyny. Oczywiście, żadne działania nie zapobiegają wszystkim awariom. Ich liczbę można jednak zmniejszyć – służą temu określone rutynowe działania:

- Stosowanie zabezpieczeń technologicznych i elektrycznych. Wybierając system zabezpieczeń, musimy pamiętać o jego cenie. Zabezpieczenia nie mogą być droższe od chronionego mienia i ewentualnych kosztów przestoju wskutek zatrzymania maszyny.
- Przeprowadzanie prawidłowej konserwacji. Wszelkie czynności eksploatacyjne należy wykonywać zgodnie z zaleceniami producenta. Harmonogram remontów powinien być sporządzony na podstawie rzetelnej oceny stanu technicznego uzależnionej od wyników badań diagnostycznych oraz własnych doświadczeń. Do remontów powinny być używane oryginalne lub certyfikowane części zamienne.
- Stosowanie diagnostyki. Badania diagnostyczne wykonywane z użyciem kamer termowizyjnych, spektrografów, endoskopów, przy pomocy

ultradźwięków i promieni RTG, dają szansę wczesnego wykrycia oznak konieczności wykonania remontu.

LICZYMY STRATY

Naprawa uszkodzonej maszyny czy zakup nowej, to nie wszystkie koszty, które trzeba ponieść. Awaria maszyny może zagrażać zdrowiu, a nawet życiu operatora. Spowoduje zatrzymanie linii produkcyjnej i, co za tym idzie, doprowadzi do niewywiązania się z umowy handlowej na dostawę wyrobów. Jeśli produkt ma być przetwarzany u odbiorcy, pojawia się ryzyko zatrzymania produkcji u partnera handlowego. Dopuszczenie do pracy maszyny niesprawnej, zwiększa odsetek wyrobów niepełnowartościowych, powoduje zmniejszenie sprzedaży i spadek rentowności zakładu. Wzrasta też liczba reklamacji składanych przez niezadowolonych klientów. W szczególnym przypadku może dojść do konieczności wycofania produktu z rynku i poniesienia odpowiedzialności za straty nabywców. Jest jeszcze jeden rodzaj strat trudnych do oszacowania: mamy z nimi do czynienia wtedy, gdy uszkodzona maszyna jest przyczyną wydostania się z instalacji technologicznej substancji chemicznej, powodującej skażenie środowiska naturalnego.

PODSUMOWANIE

Mówiąc o awariach maszyn i urządzeń, nie sposób uznać, że występują one głównie z przyczyn technicznych. Wzrasta bowiem liczba tych spowodowanych błędami obsługi. Człowiek jest słabym ogniwem procesu sterowania maszyną. Pomimo istnienia blokad technologicznych, systemów zabezpieczeń oraz obowiązujących procedur, nieprawidłowości w obsłudze mogą wystąpić w każdej chwili i spowodować poważne szkody. Nikt nie może być pewien bezawaryjnej pracy swoich maszyn. Człowiek popełnia błędy, zabezpieczenia ograniczają tylko skutki awarii. Nadzieję na poprawę tego stanu dają nowe technologie wkraczające w obszary sterowania i zabezpieczeń. Większość nowych systemów wdrażanych w przemyśle nadzoruje przebieg procesu technologicznego, by wyeliminować jego niedoskonałości. Niewątpliwie do takich należy system SCADA (ang. Supervisory Control And Data Acquisition), który zbiera, porównuje i prezentuje dane pozyskane w trakcie monitoringu urządzeń. System w szerokim zakresie jest już wykorzystywany w energetyce, przemyśle farmaceutycznym i innych branżach. Można go też łatwo i niskim kosztem dostosować do sterowania i nadzoru nad pracą maszyn i urządzeń nietypowych. Łańcuch metod, którymi można ograniczyć awaryjność maszyn, jest długi, ale tylko tak mocny, jak jego najsłabsze ogniwo. ■



Ryszard Boyke

Główny Specjalista ds. Oceny Ryzyka w Hestia Loss Control. Zajmuje się zagadnieniami ryzyka uszkodzenia maszyn i urządzeń, utraty zysku oraz ryzyka budowlano-montażowego. Absolwent Wydziału Elektrycznego Politechniki Gdańskiej, w Grupie ERGO Hestia od 1994 r., w Hestia Loss Control od 1999 r.



ryszard.boyke@ergohestia.pl



229 DNI nieświadomości

LISTOPAD 2014 TO NAJGORSZY MIESIĄC W HISTORII PRACY DZIAŁU IT FIRMY SONY PICTURES. ŚWIATOWEGO GIGANTA PRODUKCJI FILMOWEJ ZAATAKOWALI NIEZNANI SPRAWCY, PODPISUJĄCY SIĘ JAKO #GOP. SKRADLI NIEUPUBLICZNIONE JESZCZE FILMY ORAZ, CO GORSZA, POUFNE DANE PRACOWNIKÓW I CELEBRYTÓW. W EFEKCIE ZNACZNIE UCIERPIAŁY WIARYGODNOŚĆ I WIZERUNEK JAPOŃSKIEGO PRODUCENTA.

Tekst: Tomasz Dolata, Dariusz Włodarczyk



Po miesiącu śledztwa FBI ustaliło, że za atakiem stała Korea Północna. Są na to dowody. Sprawa, którą na pierwszy rzut oka można by uznać za kolejny incydent, okazała się bitwą polityczną i biznesową, a atak pogorszył już i tak złe stosunki pomiędzy Stanami Zjednoczonymi i Koreą Północną. Był to największy cios wymierzony w Sony Pictures, który pokazał, że poufne dane są niewystarczająco zabezpieczone i łatwo mogą stać się łupem dla cybernetycznych włamywaczy.

Ataki podobne do tego wymierzonego w Sony Pictures często mają tło finansowe i polityczne. Grupy hakywistów, którzy niejednokrotnie wykorzystują nieprzeciętne umiejętności w dobrze pojętym interesie społecznym, ulegają pokusie szybkiego zasilenia swoich kont bankowych. Potencjalni zleceniodawcy to instytucje aktywne na arenie politycznej, konkurujące ze sobą przedsiębiorstwa czy organizacje terrorystyczne. Tak szeroki przekrój środowisk, którym może zależeć na wywołaniu konfliktu politycznego lub załamania gospodarki, implikuje konieczność stosowania coraz lepszych zabezpieczeń nie tylko technicznych, ale przede wszystkim socjologicznych. Niech za przykład posłużą fora dyskusyjne, repozytoria i centra wymiany wiedzy, zwane potocznie ISAC (Information Sharing and Analysis Centres), dzięki którym możliwa będzie szersza wymiana informacji o atakach i sposobach ochrony. Zasilenie CERT-ów czy SOC-ów regularną dawką informacji, to duży krok w kierunku bardziej efektywnego wykorzystania zabezpieczeń technicznych.

PRZEPIS NA (H)ATAK
Zanim zaczniemy analizować konsekwencje ataku, warto zastanowić się nad tym, co w ogóle nam grozi. Czy rzeczywiście całe zło czyhające w sieci Internet lub Darknet dotyczy naszej organizacji? Przecież ostatnie inwestycje zmierzające do

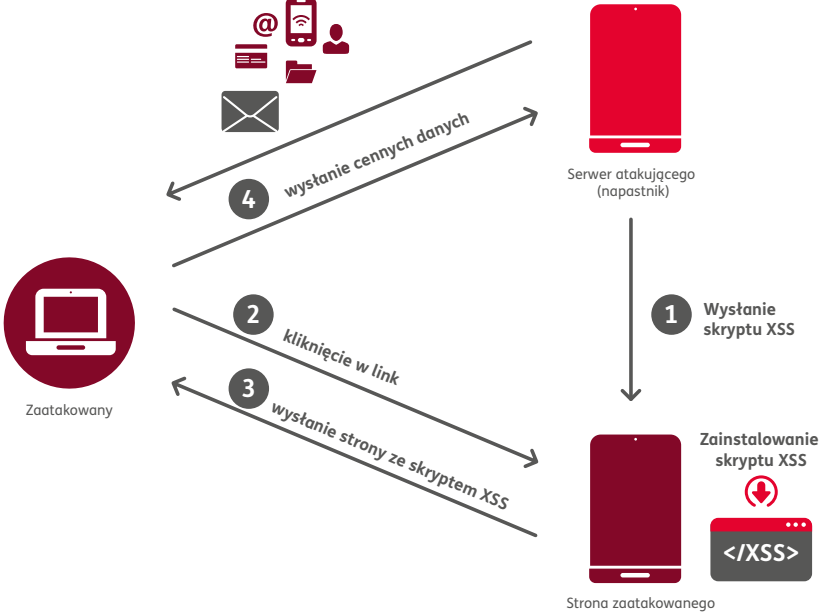
uszczelnienia punktów styku z internetem były tak duże, że nawet mysz się nie prześliznęła. Mysz faktycznie nie, ale taki mały, niewidoczny, złośliwy pakiet danych – owszem. Zdecydowanie większość działań przestępczych w „realu” czy świecie wirtualnym opiera się na planie, logice lub innej przemysłowej formie realizacji.

Krok 1. Rozpoznanie
Działanie polegające na wykorzystaniu przez atakującego informacji pozyskanych z różnych źródeł. Wszystko po to, żeby lepiej zrozumieć swoją ofiarę i sprawniej przeprowadzić kolejne kroki. Wymieniając czynności, jakie będą towarzyszyły rozpoznaniu, należy zaznaczyć, że niewątpliwie trudno je zdemaskować, gdyż są tak niewinne, że większość ofiar nie skojarzy ich z potencjalnym zagrożeniem. Bo cóż dziwnego w tym, że sprzątaczką codziennie wynosi śmieci, a kłoszard w nich grzebie? Normalne przecież jest to, że czasem zadzwoni GUS z prośbą o poświęcenie kilku minut na przeprowadzenie ogólnopolskiego badania albo student, który zada nam kilkanaście niepozornych pytań pod pretekstem zbierania materiału do pracy naukowej. Tym trudniej doszukać się czegoś nienaturalnego w tym, że za pośrednictwem portalu społecznościowego poznałimy niespotykaną sympatyczną osobę, z którą się doskonale rozumiemy i możemy porozmawiać na wszystkie tematy. Przykładów można wymienić więcej. Wspólny mianownik – socjotechnika, zwana również inżynierią społeczną. To wyrafinowany zespół technik manipulacji zmierzający do osiągnięcia postawionego celu – w tym przypadku celem jest informacja.

Krok 2. Atak
Tak, to już w drugim kroku napastnicy włamują się do sieci, wykorzystując nieprzeciętną wiedzę z obszaru teleinformatyki i, rzecz jasna, informacje, które zdobyli w kroku 1. Na tym etapie dochodzi do infekcji zasobów teleinformatycznych ofiary złośliwym oprogramowaniem. Liczba zagrożeń i ich mutacji jest liczona w milionach i z roku na rok rośnie logarytmicznie. Do sztandarowych wektorów ataku niewątpliwie należą:
SQL Injection (z ang. zastrzyk SQL) – bardzo często spotykana i jedna z najniebezpieczniejszych podatności aplikacji webowych. Należy do pierwszej kategorii (A1) błędów według OWASP (Open Web Application Security Project). Polega na wstrzyknięciu do aplikacji fragmentu zapytania SQL. Jeśli aplikacja nie ma trybu walidacji przekazywanych parametrów przez użytkownika, powoduje to przekazanie zapytania bezpośrednio do bazy SQL. Skutek? W zależności od sytuacji atakujący omija mechanizm uwierzytelnienia, otrzymując dostęp w trybie odczytu lub zapisu do całej bazy danych. Ponadto może otrzymać dostęp do plików systemu operacyjnego, na

którym pracuje baza danych, z możliwością tworzenia własnych plików i wykonywania kodu w systemie operacyjnym.
XSS (Cross-Site Scripting) – atak na klienta, który korzysta z podatnej aplikacji webowej, polegający na wstrzyknięciu do przeglądarki ofiary fragmentu JavaScriptu lub innego języka skryptowego (np. VBScript). Wykonanie kodu w przeglądarce ofiary może skutkować np. kradzieżą cookies, a tym samym przejściem aktywnej lub zalogowanej sesji ofiary, podmianą strony internetowej czy uruchomieniem Keyloggera czytającego wszystkie znaki wpisywane z klawiatury. Atak XSS ma wiele odmian, jednak na dwie z nich należy zwrócić szczególną uwagę. Są to XSS Persistent i XSS Reflected. Pierwsza, najbardziej złośliwa, polega na umieszczeniu kodu JavaScript po stronie serwerowej, np. w komentarzu pod blogowym postem. W momencie gdy moderator bloga odczytuje komentarz, kod JavaScript uruchamia się automatycznie. Skutek? Natychmiastowe przejście sesji administracyjnej bez znajomości loginu i hasła. Druga odmiana polega na umieszczeniu kodu JavaScript w linku przesyłanym do ofiary, np. w formie wiadomości e-mail. Ofiara po kliknięciu linka łączy się z aplikacją, która zwraca ofierze wynik, powodując wykonanie kodu w przeglądarce. Skutek podobny jak w przypadku XSS Persistent.

ATAK CROSS SITE-SCRIPTING
Ransomware (z ang. okup) – rodzaj oprogramowania używanego w przestępczości internetowej, którego działanie polega na wnikięciu do wnętrza atakowanego komputera i zaszyfrowaniu danych należących. Do zdarzenia może dojść np. w wyniku kliknięcia w załącznik przesyłany pocztą elektroniczną. Wówczas na ekranie zainfekowanego komputera pojawia się komunikat



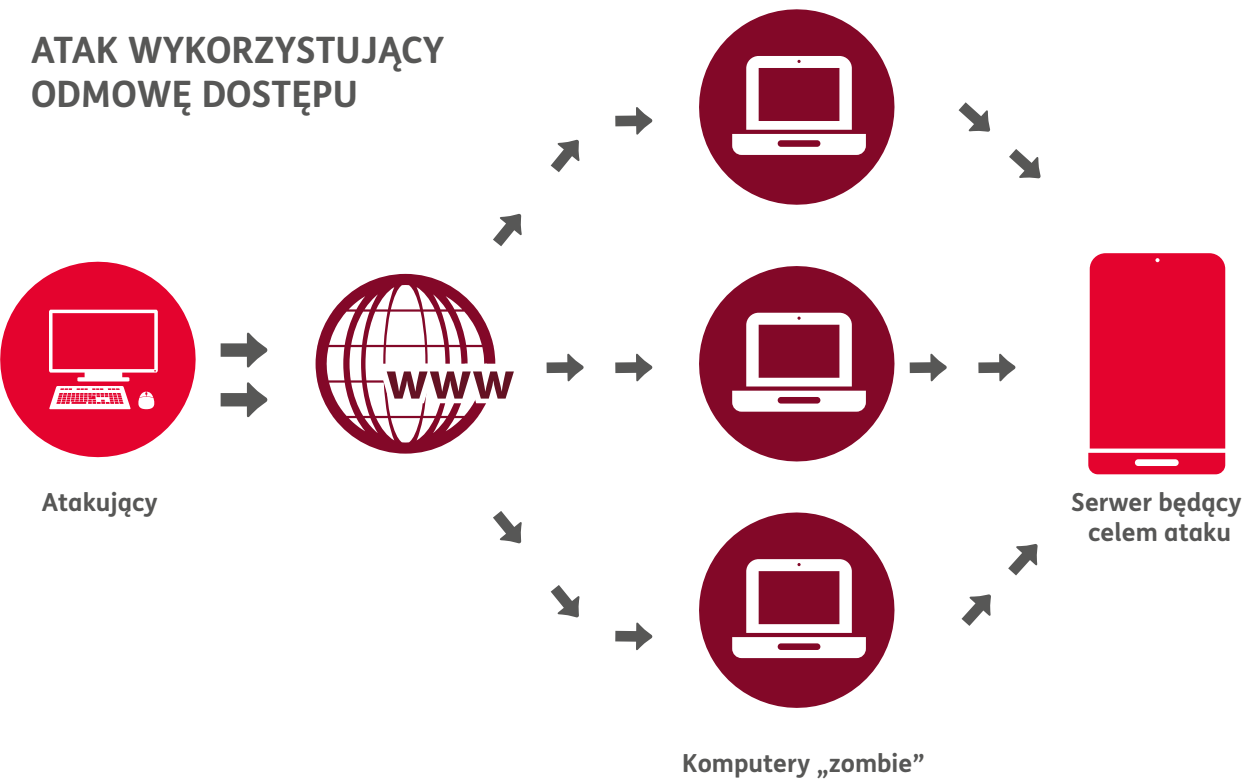
z krótką instrukcją, jak odzyskać dane. Zazwyczaj przestępca domaga się przesłania sporej sumy pieniędzy na wskazany rachunek bankowy, zobowiązując się jednocześnie do przesłania kluczy i instrukcji, jak odszyfrować dane. Czy postąpi zgodnie z taką deklaracją? Oby nikt z nas nie musiał się o tym przekonywać. Obrona przed takim zagrożeniem wydaje się bardzo prosta. Wystarczy regularnie robić kopie bezpieczeństwa danych i nie otwierać podejrzanych załączników.
0-day attack (program mający na celu wykorzystanie błędów w oprogramowaniu) – pojawia się na czarnym rynku przed publikacją poprawki przez producenta. Etyka bezpieczeństwa teleinformatycznego

(z ang. white hat), w przypadku odkrycia podatności każe poinformować o tym producenta oprogramowania, którego zadaniem jest wypuszczenie poprawki. Rzeczywistość jednak okazuje się brutalna. Często odkrywcy luki sprzedają tę informację cyberprzestępcom (z ang. black hat), którzy nie szczędząc czasu i sił, wykorzystują ją do ataków.
Malware – wszelkiego rodzaju działania, których zadaniem jest osłabienie systemu obronnego komputera ofiary poprzez instalację złośliwego oprogramowania. Chodzi tu o popularne i dobrze znane wirusy, robaki, trojany, rootkit, adware, grayware, spyware itp. Ich praca polega na gromadzeniu danych >>



Czy w Polsce, gdzie nie ma firm działających na taką skalę jak Sony Pictures, możemy czuć się bezpieczni?

Według danych podawanych przez producenta oprogramowania antywirusowego Kaspersky do państw najbardziej narażonych na cyberwłamania należą: Rosja, Stany Zjednoczone, Indie, Niemcy, Francja, Wietnam, Kanada, Meksyk, Japonia i Brazylia. Polska w tym rankingu znajduje się w czwartej dziesiątce najczęściej atakowanych krajów na świecie.



o użytkownika (tj. danych osobowych, numerów kart kredytowych, loginów, haseł, poczty, adresów stron WWW – słowem, wszystkiego), a następnie dostarczaniu ich cyberprzestępcy.

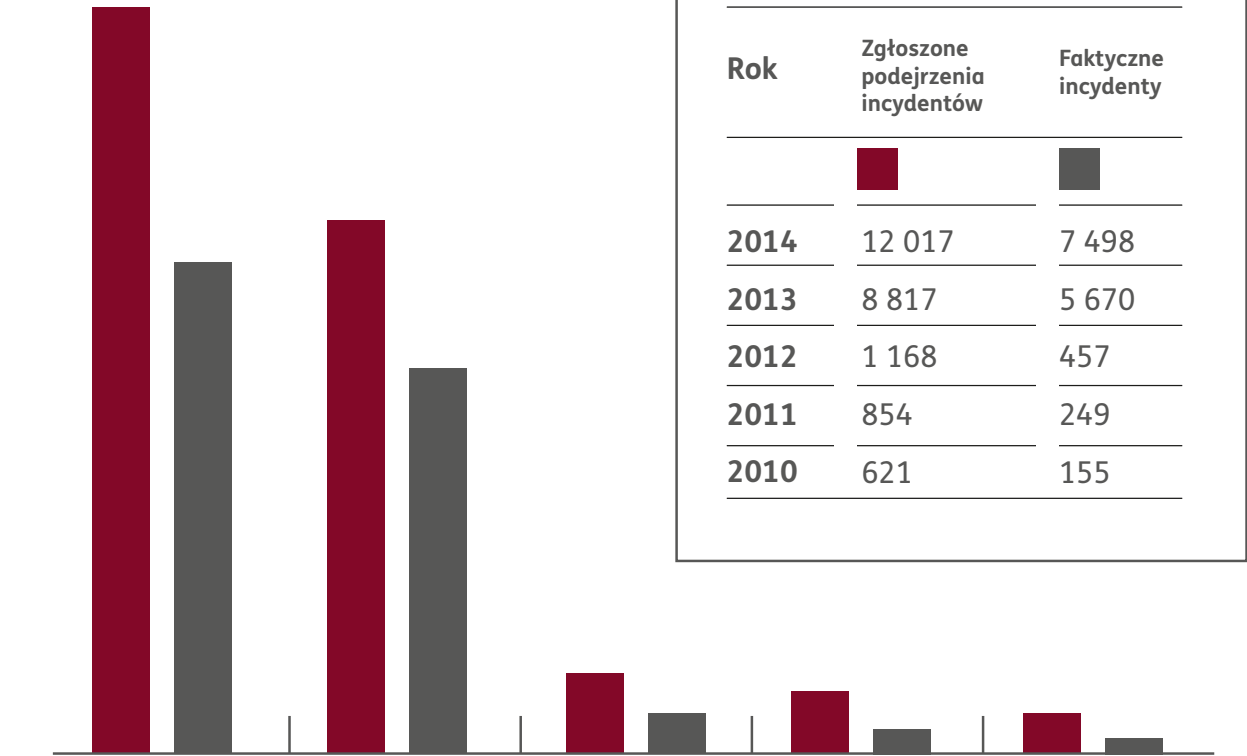
Do zdarzenia dochodzi zazwyczaj po otrzymaniu wiadomości e-mail, zawierającej zainfekowany załącznik lub link do strony, na której cyberprzestępca umieścił złośliwe oprogramowanie. Treść wiadomości nakłania w inteligentny sposób do kliknięcia w link lub rozpakowania załącznika. Niefrasobliwość użytkownika w każdym przypadku prowadzi do infekcji. Zatem należy być czujnym, czytając kolejną wiadomość o problemach z dostarczeniem przesyłki, jak również z ostrzeżeniem przed sądowym wezwaniem do zapłaty za usługę, którą niedawno zakupiliśmy.

Krok 3. Detekcja
W tym kroku atakujący penetruje sieć ofiary, zdobywając informacje o jej zasobach i zabezpieczeniach – przez cały czas ukrywając swoje działania przed okiem działu bezpieczeństwa. Ten etap jest sprawdzianem dla każdej ze stron. Naprzeciw wiedzy i umiejętnościom wykorzystania exploitów stoją ciężkie działa w postaci firewalli aplikacyjnych (WAF), sond wykrywających anomalie sieciowe (IDP) oraz korelatorów zdarzeń (SIEM), które podają

na tacy gotowy raport zagrożeń. Co z tym zrobi dział bezpieczeństwa? Na pewno zareaguje od razu, gdy tylko raport czy alert zostanie wygenerowany. Jak szybko lub późno to nastąpi, zależy od umiejętności cyberprzestępcy.

Krok 4. Pozyskiwanie informacji
To przedostatni krok, w którym ofiara traci najwięcej: najpilniej strzeżone informacje. Własność intelektualna, kody źródłowe nowych aplikacji, nieemitowane jeszcze filmy, dane do transakcji finansowych, plany rozwoju, dane do uwierzytelnienia pracowników, numery kont, informacje o transakcjach itd. Słowem: to, co może mieć wartość na rynku. Jednak pieniądze to nie wszystko, a przynajmniej nie w bezpośrednim tego słowa znaczeniu. Celem napastników często jest zakłócenie procesów funkcjonujących w przedsiębiorstwie. Przykładem mogą być elektrownie, w których atak na system SCADA (system nadzorujący proces technologiczny) może spowodować przerwę w dostawie prądu; banki, w których wyłączenie systemu transakcyjnego lub nadzorującego pracę bankomatów może wpłynąć zarówno na wizerunek, jak i wyniki finansowe; wreszcie szpitale, w których przejęcie kontroli nad urządzeniami odpowiedzialnymi za podtrzymanie życia może mieć przerażające skutki.

Ryzyko cybernetyczne



Krok 5. Zacieranie śladów
Ostatni krok to swoiste „wyjście po angielsku” z infrastruktury ofiary. Temu procesowi towarzyszy często pozostawienie ukrytego przejścia (tzw. backdoor) ułatwiającego ponowny atak. Potem następuje już tylko „analiza” danych zebranych podczas ataku.

Wnikliwi znawcy tematu rozpoznali zapewne w przepisie na (h)atak kumulację zagrożeń cybernetycznych zwaną potocznie atakiem ukierunkowanym (ang. APT – Advanced Persistent Threat). Oczywiście, skala i liczba wykonanych kroków, składających się na atak, zależą od fantazji napastnika lub zlecenia, którego się podjął.

JESTEŚMY BEZPIECZNI?
Czy w Polsce, gdzie nie ma firm działających na taką skalę jak Sony Pictures, możemy czuć się bezpieczni? Według danych podawanych przez producenta oprogramowania antywirusowego Kaspersky, do państw najbardziej narażonych na cyberwłamania należą: Rosja, Stany Zjednoczone, Indie, Niemcy, Francja, Wietnam, Kanada, Meksyk, Japonia i Brazylia. Polska w tym rankingu znajduje się w czwartej dziesiątce najczęściej atakowanych krajów na świecie (<https://cybermap.kaspersky.com/> pokazuje bieżącą sytuację dotyczącą ataków). Niedawno dość szerokim echem

w mediach odbiły się informacje o atakach hakerów na Polskie Linie Lotnicze LOT oraz Plus Bank. Z tym że serwery PLL LOT, według nieoficjalnych źródeł, miały posłużyć do ataku na inną, nieznaną firmę. Mowa tutaj o posłużeniu się serwerami do ataku DDoS, który wykorzystuje dostępną przepustowość serwera, co prowadzi do niedostępności usługi lub infrastruktury. W trakcie ataku DDoS na serwer zostaje przesłanych wiele zapytań jednocześnie, a ich liczba może doprowadzić do przerw w dostępie, a nawet do całkowitego braku połączenia z serwerem. Nie zmienia to faktu, że choć nie był to bezpośredni atak na polskiego przewoźnika lotniczego, spowodował opóźnienie lub odwołanie lotów.

DISTRIBUTED DENIAL OF SERVICE ATTACK
Ataki DDoS można scharakteryzować poprzez cztery podstawowe wektory ataku: **TCP Connection Attacks** – próby wykorzystania wszystkich dostępnych połączeń do urządzeń takich jak: firewalles, load-balancery i serwery aplikacji, które – mimo że są w stanie obsłużyć miliony połączeń – w przypadku tego ataku zostają na tyle skutecznie obciążone, że wyświetlają tylko jeden komunikat, SERVICE DOWN (z ang. odmowa usługi). **Volumetric Attacks** – próby zużycia dostępnego pasma w sieci docelowej

(atakowanej) lub pomiędzy takimi sieciami a internetem. W wyniku tego ataku, powstają zatory powodujące olbrzymie spowolnienie działających usług oraz drastyczne obniżenie przepustowości sieci.

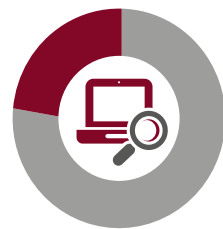
Fragmentation Attacks – wysłanie fragmentów pakietów TCP lub UDP do infrastruktury ofiary. W obliczu fali podzielonych danych, zaatakowany serwer nie jest w stanie złożyć kompletnego strumienia pakietu po swojej stronie, w związku z czym spada jego wydajność aż do całkowitej niedostępności.

Application Attacks – ataki kierowane bezpośrednio w aplikację, a dokładnie w konkretną usługę. Specyfika i skuteczność tego ataku polega na tym, że może być przeprowadzony z niewielu maszyn atakujących, które generują niskie natężenie ruchu sieciowego, tym samym są bardzo trudne do wykrycia i unieszkodliwienia.

HAKERSKIE OCZEKIWANIA
O wiele bardziej spektakularny był atak wymierzony bezpośrednio w Plus Bank. Haker Polsilver złamał zabezpieczenia i wykradł poufne dane klientów banku: imię i nazwisko, PESEL, numer dowodu osobistego, adres, historię 50 ostatnich transakcji, informacje o lokatach i kredytach, a także dane kart płatniczych i kredytowych. Włamywacz zażądał 200 tys. zł okupu, w przeciwnym razie miał

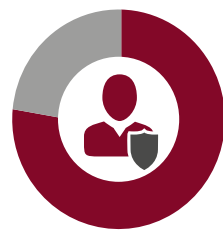


Jak wykrywane są zagrożenia?

**33%**

ofiar odkryto atak cybernetyczny dzięki wewnętrznej kontroli

Spadek wykrywalności z 37% w porównaniu z 2012 r.

**67%**

ofiar dowiedziało się o ataku dzięki informacjom z zewnątrz

Czas, jaki upłynął między potwierdzonym wystąpieniem zagrożenia, a jego wykryciem

**229**

to średnia liczba dni, w których grupy dokonujące ataku były obecne w sieci ofiary, zanim zostały wykryte

Spadek o 14 dni w porównaniu z 2012 r.

Najdłuższa niewykryta obecność: 2287 dni

upublicznić skradzione dane. Bank ostatecznie nie spełnił żądań i dane kilkuset klientów zostały udostępnione w internecie. Wówczas atakujący postawił bankowi ultimatum, gdyż – jak utrzymywał – nie chciał, aby wskutek błędów Plus Banku cierpieły osoby prywatne. Tym razem zażądał 200 tys. zł na dom dziecka. Wpłata miała zapobiec dalszemu upublicznianiu wykradzionych danych, które haker faktycznie posiadał.

Są to oczywiście przykłady ataków na jedno z największych polskich przedsiębiorstw, co nie oznacza, że tylko takie będą w najbliższej przyszłości zagrożone. Trzeba liczyć się z tym, że duże przedsiębiorstwa przeznaczają spore nakłady finansowe na bezpieczeństwo sieci. Trudniej je więc atakować. Ostatnio pojawiły się przykłady ataków hakerów na mniejsze firmy, np. na kancelarię prawną. Taki cel jest atrakcyjny ze względu na liczbę posiadanych danych osobowych. Cyberprzestępstwa nie służą hakerom tylko do zdobycia sławy, ale również do uzyskania korzyści finansowych. W przypadku Plus Banku haker żądał okupu, natomiast w wielu przypadkach jest tak, że sprzedaje on skradzione dane, np. na forum ToRePublic.

Nielegalny obrót informacją to od dłuższego czasu zjawisko powszechne i wysoce opłacalne. W „podziemiach internetu” (tzw. Darknet lub ToR) kwitnie handel skradzionymi danymi, szkodliwym oprogramowaniem czy też hostingiem zasobów informacyjnych, służącym do przeprowadzenia ataku. Wyobraźmy sobie taką sytuację: cyberprzestępca przeszukuje ogłoszenia w sieci ToR, wybiera z nich jedno, które oferuje sprzedaż aplikacji. Po zakupie zaczyna w niej budować własne oprogramowanie

(tzw. virus builder). Służy ono do ataku np. na konkretną wybraną wersję Windows OS, wybraną wersję przeglądarki internetowej itd. W cenie zakupu może być również opcja wsparcia serwisowego w przypadku „jakichkolwiek problemów” z obsługą oprogramowania. Następnie infekuje komputer ofiary, a wstrzyknięte oprogramowanie wykrada dla niego cenne informacje, przesyłając je do wskazanego w internecie zasobu. Kolejnym krokiem jest już wspomniany wcześniej obrót w celach zarobkowych, i tak ceny w przypadku kradzieży poniższych danych kształtują się następująco (wybrane dane z raportu Symantec):

- 1000 skradzionych adresów e-mail – 0,50-10 dol.
- 1 mln zweryfikowanych adresów e-mail – 70-150 dol.
- dane karty kredytowej – 0,50-20 dol.
- skradziona tożsamość w grach komputerowych – 10-15 dol.
- skan prawdziwego paszportu – 1-2 dol.
- zarejestrowana i aktywna karta SIM (dotyczy telefonów w Rosji) – 100 dol.
- spersonalizowany malware – 12-3500 dol.

Jak pokazują dane CERT, czyli rządowego zespołu zajmującego się bezpieczeństwem sieci, liczba incydentów w Polsce z roku na rok zwiększa się. Szczególnie wzrosła w ostatnich dwóch latach.

W dobie technologicznego rozwoju ataki crackerskie stają się normalnością. Polskie firmy powinny odpowiedzieć sobie na kilka ważnych pytań. Czy jesteśmy świadomi zagrożenia? Jak jesteśmy na nie przygotowani i przed nimi zabezpieczeni? Inną kwestią pozostaje ustalenie przyczyn i skutków ataku, a więc działania związane z informatyką śledczą. Średni czas

wykrycia ataku hakerskiego wynosi 229 dni, a zdarzały się przypadki, kiedy grupa włamywaczy była obecna w sieci informacyjnej poszkodowanego ponad 2 tys. dni! Wynika to z faktu, że aż 67 proc. zaatakowanych firm dowiaduje się o ataku dopiero od... hakerów, którzy po prostu sami się ujawniają.

CO NAS CZEKA?

Najbliższa przyszłość związana z cyberryzykiem w szczególności będzie dotyczyła ochrony przed zagrożeniami i wymuszeniami online. Nowe techniki ataku będą się raczej skupiały na zrozumieniu logiki systemu niż na technicznych aspektach operacji. Atakujący będzie upatrywał sukcesu, pośrednio wywołując strach swojej ofiary przed utratą danych. Będzie również wykorzystywać jeszcze bardziej dojrzałe i wyrafinowane elementy socjotechniki. Pozyskana wiedza na temat działalności gospodarczej i logiki systemu danego przedsiębiorcy, pozwoli na zamaskowanie działających w tle złośliwych kodów wrogich aplikacji. A wszystko po to, aby wyłudzić pieniądze za utracone dane, tym samym pozbawić ofiarę dobrego wizerunku.

Kolejnym zagrożeniem niedalekiej przyszłości z pewnością będą wszelkiej maści urządzenia inteligentne, m.in. drony, samochody oraz urządzenia gospodarstwa domowego podłączone do internetu (tzw. Internet of Things, IoT). Szacuje się, że liczba tych ostatnich wzrośnie o blisko 67 proc., w ciągu najbliższych pięciu lat. Tym bardziej niepokojące jest, że różnorodność systemów operacyjnych oraz brak regulacji w zakresie chociażby bezpieczeństwa IT tych urządzeń, daje możliwość wykazania się cyberprzestępcom. Podobnie wygląda kwestia opracowania regulacji w zakresie produkcji i eksploatacji dronów, które mogą być wykorzystane do naruszenia przestrzeni powietrznej, co stanowi zagrożenie dla lotnictwa, jak również to, że drony mogą zastąpić, np. bojowników ISIS w samobójczych atakach terrorystycznych.

Ochrona urządzeń mobilnych – w tym transakcji płatniczych, które większość społeczeństwa realizuje tą metodą – to kolejny element układanki, którego pominąć nie sposób. Dynamiczna implementacja systemów płatności mobilnych jest ciągłą inspiracją do prac nad oprogramowaniem wykradającym dane kart kredytowych, wykonanych w technologii EMV (zawierające chip elektroniczny) czy RFID (tzw. zbliżeniowe). Na celowniku są również mobilne portfele oferowane przez Apple czy Google Wallet Pay. Badanie przeprowadzone w Chinach, gdzie są dostępne platformy innych producentów niż chociażby w Europie i Ameryce Północnej, oraz różnorodność serwisów oferujących bezpłatne pliki do pobrania dowodzi, że trzy z czterech aplikacji są złośliwym oprogramowaniem.

Prognoza wzrostu ilości szkodliwego oprogramowania do końca 2016 r. sięga 20 mln. Pocieszająca wydaje się sytuacja w innych krajach, w których użytkownicy zazwyczaj zwracają się do oficjalnych sklepów z aplikacjami.

Zdziwienie wielu użytkowników popularnych platform mobilnych może wywołać raport Symantec sporządzony na podstawie badań przeprowadzonych w Ameryce Północnej. Według niego procentowy rozkład liczby zagrożeń na systemy operacyjne przedstawia się następująco:

- iOS – 84 proc.
- Android – 11 proc.
- BlackBerry – 4 proc.
- Windows Phone – 1 proc.

Sondowanie zmian dotyczy również personelu odpowiadającego za analizę i przeciwdziałanie zagrożeniom cybernetycznym. Większość przedsiębiorstw coraz bardziej uświadamia sobie potrzebę zapewnienia integralności danych wewnątrz i na zewnątrz swoich zasobów. Obecne trendy dążą do powołania stanowisk Data Protection Officer oraz Risk Officer, czyli osób nadzorujących bezpieczeństwo danych i analizę ryzyka w kontekście zapewnienia integralności oraz zgodności z przepisami obowiązującymi w kraju, w którym dane

są przechowywane. Wysoka świadomość dotycząca ochrony danych spowoduje zmianę mentalności organizacji oraz pozwoli opracować strategię wobec ataków cybernetycznych.

UBEZPIECZONE CYBERRYZYKO?

Cyberryzyko to również wyzwanie dla ubezpieczycieli, którzy w swojej ofercie mają lub w najbliższej przyszłości będą mieć produkt ubezpieczeniowy, chroniący w przypadku działalności hakerów i wirusów komputerowych. Z tych wyzwań największe dotyczy likwidacji szkody. Chodzi tutaj zarówno o czas reakcji, tak aby jak najszybciej usunąć zagrożenie, żeby nie dochodziło do dalszych szkód, jak i określenie, kiedy do ataku doszło i czy ubezpieczyciel za taki atak odpowiada. Jak wskazano wcześniej, od momentu ataku do jego wykrycia mijają miesiące, czasami lata, więc okres ubezpieczenia może takich zdarzeń nie obejmować.

Dla klientów z kolei najważniejsze będą zakres ubezpieczenia i koszty, które zostaną pokryte. Przygotowanie optymalnego produktu wymaga czasu, ale również jego dalszy rozwój powinien być dobrze zaplanowany. Jedno nie ulega wątpliwości: liczba cyberzagrożeń będzie rosła, gdyż wiąże się to z coraz większą informatyzacją.

**Tomasz Dolata**

Specjalista ds. Ubezpieczeń w Biurze Ubezpieczeń Podmiotów Gospodarczych. Zajmuje się ubezpieczeniami majątkowymi, technicznymi oraz budowlano-montażowymi. Absolwent Akademii Morskiej w Gdyni. W Grupie ERGO Hestia od 2007 r.



tomasz.dolata@ergohestia.pl

**Dariusz Włodarczyk**

Główny Specjalista ds. Oceny Ryzyka Cyber w Hestia Loss Control. Zajmuje się problematyką szeroko pojętego cyberbezpieczeństwa. Absolwent Wydziału Mechanicznego Politechniki Gdańskiej. W Grupie ERGO Hestia od 2015 r.



dariusz.wlodarczyk@ergohestia.pl

SZKOLENIA

– lekarstwo dla floty

CZY SZKOLENIA FLOTOWE SĄ POTRZEBNE? JAKĄ ROLĘ ODGRYWAJĄ W EFEKTYWNYM ZARZĄDZANIU FLOTĄ? CZEGO I KOGO POWINNY DOTYCZYĆ?

Tekst: Piotr Lipiński

Jeżeli jesteś mężczyzną w wieku 20-34 lat, który kieruje samochodem osobowym przy dobrych warunkach atmosferycznych w lipcowy lub wrześniowy piątek, strzeż się wypadku – tak zaczęło się jedno ze szkoleń bezpiecznej jazdy dla kierowców flot samochodowych. Pozornie przekorne twierdzenie, opracowane na podstawie statystyk Krajowej Rady Bezpieczeństwa Ruchu Drogowego, zasiało nutę niepewności, a zarazem ciekawości i rozpętało wśród obecnych na szkoleniu kierowców zagorzałą dyskusję o bezpieczeństwie jazdy. Temat okazał się na tyle absorbujący, że czas szkolenia wydłużył się dwukrotnie, a uczestnicy bez wahania zadeklarowali chęć uczestnictwa w kolejnych kursach. Czy szkolenia flotowe są potrzebne? Jaką rolę odgrywają w efektywnym zarządzaniu flotą? Czego i kogo powinny dotyczyć?

RYZYKO

Posiadanie własnej floty samochodowej generuje ryzyko dla przedsiębiorstwa. Stan infrastruktury drogowej, stan techniczny pojazdów i ich wyposażenie, umiejętności kierowców, polityka flotowa przedsiębiorstwa – to tylko niektóre czynniki wpływające na ryzyko wystąpienia zdarzeń niepożądanych, takich jak tzw. szkoda parkingowa, kolizja czy wypadek drogowy. Świadome zarządzanie ryzykiem polega na systematycznym analizowaniu wspomnianych czynników i wprowadzaniu działań zapobiegających wystąpieniu zdarzeń niepożądanych. Bo kiedy do nich dojdzie, przedsiębiorstwo poniesie straty finansowe i wizerunkowe. Nadszarpnięte zostanie również zaufanie ze strony pracowników. Właściwe podejście do oceny ryzyka floty to podejście holistyczne. Flotę samochodową należy

traktować jak jeden organizm. Dysfunkcję jednego organu „leczyć” z uwzględnieniem całego układu.

BEZPIECZNA FLOTA

„Zdrowa” flota to bezpieczna flota, a więc niska szkodowość i niższe koszty. Dlatego tak istotne jest opracowanie i wdrożenie systemu bezpieczeństwa. Świadome zarządzanie bezpieczeństwem floty zaczyna się już na etapie zakupu samochodów. Wyposażenie pojazdów w nowoczesne systemy bezpieczeństwa czynnego może znacznie ograniczyć ryzyko kolizji i wypadku drogowego. Dostępne systemy bezpieczeństwa realizują funkcję ostrzegawczą i wykonawczą. Ta pierwsza dotyczy m.in. rozpoznawania znaków drogowych, ostrzegania przed niezamierzoną zmianą pasa ruchu, kolizją, pojazdem znajdującym się



w martwym polu kierującego czy zbliżającym się z tyłu. Systemy realizujące funkcję wykonawczą pozwalają automatycznie utrzymywać stałą odległość od pojazdu poprzedzającego, zatrzymać samochód, kiedy ten najeżdża na przeszkodę, a kierowca nie reaguje na zagrożenie. Mogą nawet same parkować. Świadome zarządzanie bezpieczeństwem floty to optymalny wybór systemów z zachowaniem dbałości o bezpieczeństwo kierowców i finanse przedsiębiorstwa.

Dobrze zaprojektowane szkolenie powinno wynikać wprost z przeprowadzonej analizy i identyfikacji potrzeb szkoleniowych.

SYSTEM BEZPIECZEŃSTWA FLOTY

System bezpieczeństwa floty samochodowej należy wdrażać w odpowiednim porządku, w czterech logicznie z sobą powiązanych etapach: wywiadu, diagnozy, działań naprawczych i monitorowania.

KROK 1. WYWIAD

Istotnym elementem w procesie wdrożenia jest zbieranie informacji o stanie

bieżącym floty. Na tym etapie pozyskuje się szczegółowe dane dotyczące szkodowości, wykroczeń popełnianych przez użytkowników pojazdów, przyczyn zdarzeń drogowych, kosztów likwidacji szkód czy kosztów bieżących utrzymania ruchu pojazdów. Ponadto etap ten służy pozyskaniu informacji na temat nieformalnie przyjętych praktyk i zasad postępowania w zakresie użytkowania oraz obsługi floty samochodowej, co może mieć znaczący wpływ na budowanie i korygowanie polityki bezpieczeństwa floty.

KROK 2. DIAGNOZA

Kolejnym etapem procesu jest analiza zebranych informacji, w celu określenia czynników ryzyka i identyfikacji zagrożeń oraz wyznaczenie obszarów wymagających wdrożenia działań naprawczych. Jako najczęstszy czynnik wysokiego ryzyka, wskazuje się prawdopodobieństwo wystąpienia kolizji drogowej i wypadku drogowego. Według statystyk Komendy Głównej Policji w Polsce w 2014 r. doszło do 34 970 wypadków drogowych oraz 348 028 kolizji drogowych, przy czym aż 82 proc. wypadków drogowych wynikało z winy kierujących. W następstwie tych zdarzeń rannych zostało 42 545 osób, a 3202 osoby zmarły. Poszkodowanych zostało więc więcej ludzi, niż jest mieszkańców Sopotu! Należy zauważyć, że statystyki dotyczące liczby kolizji obrazują

wyłącznie te zdarzenia, do których wezwano patrol policji, a więc w rzeczywistości mogło być ich znacznie więcej. Wypadek drogowy niesie za sobą nie tylko straty społeczne, ale również ekonomiczne. Straty ekonomiczne obejmują m.in. koszty utraconych korzyści, utraconego mienia, akcji ratowniczych, działań medycznych, odszkodowań, koszty administracyjne itp. Łączne koszty zdarzeń drogowych w Polsce w 2013 r. zostały oszacowane przez Instytut Badawczy Dróg i Mostów na 49,1 mld zł. Koszt jednostkowy wypadku drogowego to 953 tys. zł, kolizji drogowej – 41,8 tys. zł, ofiary śmiertelnej – 1,97 mln zł, ciężko rannej – 2,21 mln zł, a ofiary lekko rannej – 30,4 tys. zł. Szacuje się, że łączne koszty zdarzeń drogowych w 2015 r. mogą wynieść około 50,7 mld zł. Oznacza to, że zdarzenia drogowe będą w tym roku kosztować każdego Polaka 1,3 tys. zł. Wskazane koszty nie zawierają jednak obciążeń przedsiębiorstwa związanych m.in. ze wzrostem składki ubezpieczeniowych na skutek wyższej szkodowości floty. W dużym uproszczeniu można stwierdzić, że im wyższa liczba szkód i wartość odszkodowania, tym większa składka ubezpieczeniowa. Z ekonomicznego punktu widzenia prawidłowa diagnoza stanu floty jest więc podstawą do opracowania działań mających obniżyć koszty jej funkcjonowania – w tym kwotę składki ubezpieczeniowej.

fot.: Dollarphotoclub.com

Właściwe podejście do oceny ryzyka floty to podejście holistyczne.

KROK 3. DZIAŁANIA NAPRAWCZE

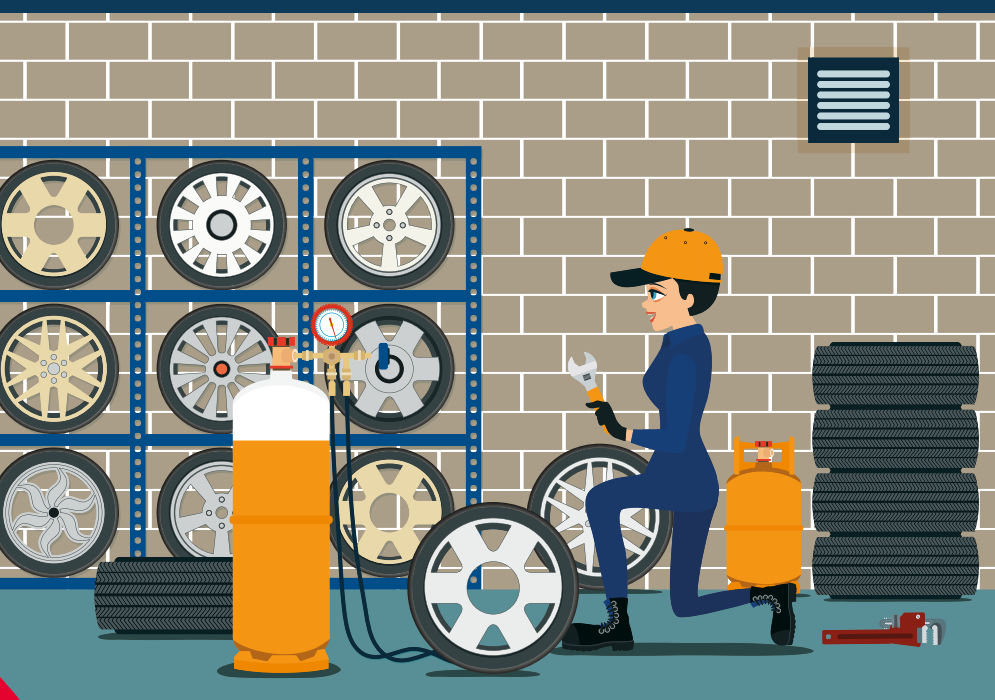
Podstawowym elementem działań naprawczych są odpowiednio dobrane szkolenia, skierowane zarówno do użytkowników pojazdów, jak i menedżerów floty. Efektywny system szkoleń skutkuje poprawą jakości funkcjonowania organizacji, a także pozwala uniknąć zdarzeń niepożądanych. Poprawia wyniki osiągane przez pracowników, ogranicza straty i sprzyja identyfikacji pracowników z organizacją. Szkolenia przynoszą zatem korzyści zarówno ekonomiczne, jak i społeczne. Za podstawowy wyznacznik dobrze zorganizowanego i zaplanowanego szkolenia, przyjmuje się tzw. metodę SMART (Simple, Measurable, Achievable, Relevant, Timely defined), która charakteryzuje odpowiednio uniwersalne cele każdego szkolenia. Cel szkolenia powinien być prosty, zrozumiały i konkretny. Należy go tak sformułować, by można było zmierzyć stopień jego realizacji. Ponadto powinien być osiągalny oraz przydatny, a także ambitny i istotny, a jego realizacja osadzona w ramach czasowych. Dobrze zaprojektowane szkolenie

powinno wynikać wprost z przeprowadzonej analizy i identyfikacji potrzeb szkoleniowych. Przygotowane na podstawie tak sformułowanych celów, będzie efektywne i przydatne dla uczestników.

DLA MENEDŻERA FLOTY

Obecnie proponuje się, by szkolenia adresowane do menedżerów floty dotyczyły obszarów związanych z jej bezpieczeństwem, finansowaniem, ubezpieczeniem, a także zastosowania nowych technologii. Za szczególnie istotne uważa się szkolenia, uwzględniające systemy telemetryczne. W zakresie zarządzania bezpieczeństwem prowadzi się kursy opracowywania, korygowania i wdrażania polityki bezpieczeństwa floty. Wskazuje się również na korzyści wynikające z zastosowania technologii telemetrycznych, takich jak możliwość kontroli sposobu jazdy kierowców. Systemy te umożliwiają analizę parametrów ruchu pojazdu, m.in. siły bezwładności podczas przyspieszania i hamowania, prędkości pojazdu czy poziomu





obrotów silnika. Dostępne parametry menedżer floty może wykorzystywać do określenia sylwetki kierowcy, a także stylu jazdy i na tej podstawie projektować programy oceny oraz premiowania bezpiecznych kierowców. Zastosowanie systemów telemetrycznych owocuje obniżeniem kosztów funkcjonowania floty czy zwiększeniem efektywności pracy poprzez optymalne planowanie tras przejazdu i zarządzanie czasem pracy kierowców. Nowoczesne systemy umożliwiają prowadzenie monitoringu przewożonego towaru, a tym samym pozwalają szybko reagować na zarejestrowane nieprawidłowości i ograniczać ryzyko straty finansowej.

DLA KIEROWCY

W grupie kierowców proponuje się szkolenia mające na celu obniżenie szkodowości floty, m.in. kursy bezpiecznej jazdy, postępowania w razie wypadku, a ostatnio

również szkolenia z zasad ekologicznej jazdy. W ramach nauki bezpiecznej (defensywnej) jazdy stosuje się rozwiązania hybrydowe, tj. szkolenia składające się z części teoretycznej oraz praktycznej. Ich celem jest wykształcenie u kierowców zdolności przewidywania i zapobiegania niebezpiecznym sytuacjom na drodze. W części teoretycznej kierowcom przedstawia się wagę problemu wypadków drogowych, ich następstwa i koszty – również społeczne – a także zasady bezpiecznego ruchu drogowego. Szczególną uwagę zwraca się na zagadnienia związane z zachowaniem bezpiecznego odstępu od pojazdu poprzedzającego, prędkością i płynnością jazdy dopasowaną do aktualnych warunków drogowych, jak również techniką manewru wyprzedzania. Niezwykle istotną częścią szkolenia jest praktyczna nauka jazdy defensywnej – kierowcy mogą w kontrolowanych warunkach drogowych doskonalić umiejętności nagłego omijania przeszkody, jazdy i hamowania na śliskiej nawierzchni, prawidłowego i efektywnego wykorzystywania systemów bezpieczeństwa, a także ćwiczyć reakcję na uślizg pojazdu. Uzupełnieniem szkolenia bezpiecznej jazdy może być zastosowanie symulatorów dachowania pojazdem, trenerów szybkości reakcji kierowców, symulatorów zdarzenia, potrącenia pieszego czy wybuchu poduszek powietrznych oraz pokaz ratownictwa i pierwszej pomocy. Elementy te

określa się mianem „edukacji rozrywkowej” (z ang. edutainment). Zastosowanie symulatorów, oprócz oczywistego charakteru edukacyjnego, pełni funkcję rozrywkową i jest coraz częściej wykorzystywaną formą zarówno podczas szkoleń, jak i spotkań firmowych. Przygotowując szkolenie z uwzględnieniem części rozrywkowo-edukacyjnej, należy jednak pamiętać, że powinna ona występować wyłącznie w charakterze uzupełnienia.

Jako związane pośrednio z bezpieczną jazdą proponuje się szkolenie z ekologicznej jazdy. O znaczeniu ekologicznej jazdy może świadczyć fakt, że jest ona jednym z elementów egzaminu na prawo jazdy, a zatem wpisuje się w politykę Unii Europejskiej dotyczącą ograniczenia emisji CO₂ w ruchu drogowym. Oprócz aspektu ekologicznego, a tym samym korzyści finansowych dla przedsiębiorstwa (mniejsze koszty paliwa to niższe koszty użytkowania floty) szkolenia z ekologicznej jazdy dotyczą tematu bezpiecznej jazdy. Kierowcy są edukowani w obszarach dotyczących przewidywania sytuacji na drodze, efektywnego wykorzystywania przełożenia czy np. oporów ruchu pojazdu związanych z odpowiednim ciśnieniem w oponach, a także z rozmieszczeniem i zabezpieczeniem bagażu, co również stanowi element przygotowania pojazdu do bezpiecznej jazdy. Ponadto kierowców szkoli się z zasad postępowania w razie zaistnienia kolizji lub wypadku

fat.: Dollarphotoclub.com

Flotę samochodową należy traktować jak organizm, a dysfunkcję jednego organu „leczyć” z uwzględnieniem całego układu.

drogowego. Podjęte przez nich działania na miejscu zdarzenia, mają na celu zmniejszenie szkody i są istotnym elementem polityki bezpieczeństwa floty. Co więcej, kierowcy są szkoleni z zasad postępowania w obszarze organizacji i udzielania pierwszej pomocy poszkodowanym.

KROK 4. MONITOROWANIE

Wdrożenie systemu bezpiecznej floty wymaga prowadzenia ciągłych działań kontrolno-naprawczych. System ten będzie skuteczny wyłącznie przy regularnej analizie wyników prowadzonych działań, ich interpretacji i – w razie konieczności – wprowadzaniu działań naprawczych. Można więc stwierdzić, że system bezpieczeństwa floty jest zapętleniem wszystkich opisanych kroków, a skuteczne działanie na rzecz bezpieczeństwa, to proces ciągły i niewyczerpany.

PODSUMOWANIE

Próżno szukać rozwiązań całkowicie eliminujących ryzyko związane z użytkowaniem floty. Jeszcze takich nie wynaleziono. Istnieją jednak narzędzia pozwalające ograniczyć ryzyko do minimum. Wśród nich istotną rolę odgrywają szkolenia. Odpowiednio dobrane i opracowane, przyczyniają się do zwiększenia bezpieczeństwa ruchu drogowego, zmniejszenia kosztów funkcjonowania floty, jak również do wzrostu zaufania pracowników do firm.



Piotr Lipiński

Specjalista ds. Oceny Ryzyka w Hestia Loss Control, wcześniej pracownik Działu Rzeczoznawców oraz Działu Ekspertyz i Kontroli Technicznych. Absolwent Wydziału Zarządzania i Ekonomii Politechniki Gdańskiej oraz Instytutu Eksploatacji Pojazdów i Maszyn Wydziału Mechanicznego Politechniki Radomskiej. W Grupie ERGO Hestia od 2010 r.



piotr.lipinski@ergohestia.pl

PRACOWNIK potrzebny od zaraz

AGENCJA PRACY TYMCZASOWEJ, PRACOWNIK TYMCZASOWY I PRACODAWCA UŻYTKOWNIK – TRZY PODMIOTY BIORĄ UDZIAŁ W REALIZACJI PRACY TYMCZASOWEJ. JAKIE PRAWA I OBOWIĄZKI MA KAŻDY Z NICH? NA CZYM POLEGAJĄ ŁĄCZĄCE JE UMOWY? I WRESZCIE: KTO ZA CO ODPOWIADA, JEŚLI PODCZAS ŚWIADCZENIA PRACY TYMCZASOWEJ DOJDZIE DO SZKODY?

KWESTIE ODPOWIEDZIALNOŚCI SĄ TU BARDZO ZŁOŻONE. POPATRZMY NA NIE OD STRONY PRAKTYCZNEJ: KTÓRY Z PODMIOTÓW BĘDZIE OBARCZONY ODPOWIEDZIALNOŚCIĄ, JEŚLI PRACOWNIK TYMCZASOWY PRZY WYKONYWANIU POWIERZONEJ MU PRACY:

- USZKODZI OBSŁUGIWANE URZĄDZENIE NA SKUTEK JEGO NIEDBAŁEGO UŻYWANIA?
- UKRADNIE CZĘŚCI SAMOCHODOWE PODCZAS PAKOWANIA ICH DO WYSYŁKI?
- USZKODZI POJAZD OSOBY TRZECIEJ PODCZAS WYŁADUNKU TOWARU?
- ULEGNIE WYPADKOWI PRZY PRACY I DOZNA USZCZERBKU NA ZDROWIU?

SCENARIUSZE POKAZĄ, ŻE W ZALEŻNOŚCI OD STOSUNKU PRAWNEGO ŁĄCZĄCEGO STRONY I RODZAJU SZKODY ODPOWIEDZIALNOŚĆ BĘDZIE SIĘ ROZKŁADAĆ INACZEJ.

Tekst: Agata Kowalczyk

Instytucja pracy tymczasowej narodziła się w Stanach Zjednoczonych. Tę formę zatrudnienia zaczęto tam wykorzystywać na początku lat pięćdziesiątych XX w. Kraje europejskie szybko doceniły profity płynące z tego proceduru i zaczęły go powielać. W latach siedemdziesiątych nadano pracy tymczasowej ramy prawne. W Polsce takie formy zatrudnienia zaczęto stosować w latach dziewięćdziesiątych ubiegłego wieku. Jednak dopiero od 2003 r., kiedy w odpowiedzi na potrzeby rynku pracy i pracodawców poszukujących innych, nowych form zatrudnienia ustawodawca zaproponował ustawę o zatrudnianiu pracowników tymczasowych, nastąpił jej dynamiczny i trwający do dziś rozwój.

CZYM JEST PRACA TYMCZASOWA?

W dużym uproszczeniu można powiedzieć, że praca tymczasowa jest nietypową formą zatrudnienia, która ma na celu zaspokajanie okresowych potrzeb pracodawców. Podstawowym aktem prawnym regulującym zagadnienie pracy tymczasowej jest Ustawa z dnia 9 lipca 2003 r. o zatrudnianiu pracowników tymczasowych (zwana dalej Ustawą), która reguluje zasady zatrudniania pracowników tymczasowych

przez pracodawcę będącego agencją pracy tymczasowej oraz zasady kierowania tych pracowników i osób niebędących pracownikami agencji pracy tymczasowej do wykonywania pracy tymczasowej na rzecz pracodawcy użytkownika.

Ustawa definiuje pojęcie pracy tymczasowej i jasno określa, w jakich sytuacjach uzasadnione jest korzystanie z pracowników tymczasowych. Art. 2 pkt 3 Ustawy stanowi, że praca tymczasowa to wykonywanie na rzecz danego pracodawcy użytkownika, przez okres nie dłuższy niż wskazany w umowie, zadań:

- o charakterze sezonowym, okresowym, doraźnym lub
- których terminowe wykonanie przez pracowników zatrudnionych przez pracodawcę użytkownika nie byłoby możliwe lub
- których wykonanie należy do obowiązków nieobecnego pracownika zatrudnionego przez pracodawcę użytkownika.

W pierwszym przypadku dobrym przykładem może być sezonowa praca przy zbiorach owoców. Drugi dotyczy chociażby takiej sytuacji, w której pracodawca

użytkownik na skutek większego niż zwykle zamówienia na swoje produkty nie jest w stanie, siłami własnych pracowników, terminowo zrealizować zamówienia. W trzeciej grupie mowa o wszelkich przypadkach zastępstw pracownika nieobecnego w pracy z powodu choroby czy dłuższego urlopu. Praca tymczasowa jest wówczas alternatywą dla umowy o zastępstwo.

Korzystanie z pracy tymczasowej podlega ograniczeniom z uwagi na ochronę zdrowia, życia lub interesów pracowników. Dlatego w myśl art. 8 Ustawy nie może być ona powierzana:

- gdy jest szczególnie niebezpieczna w rozumieniu przepisów wydanych na podstawie art. 237¹⁵ Kodeksu pracy;
- na stanowisku, na którym jest zatrudniony pracownik pracodawcy użytkownika, w okresie jego uczestniczenia w strajku;
- na stanowisku, na którym, w okresie ostatnich 3 miesięcy poprzedzających przewidywany termin rozpoczęcia wykonywania pracy tymczasowej, był zatrudniony pracownik pracodawcy użytkownika, z którym został rozwiązany stosunek pracy z przyczyn nie dotyczących pracowników.



fot.: Dollarphotoclub.com





TRZY PODMIOTY, DWIE UMOWY

Ustawa o zatrudnianiu pracowników tymczasowych wprowadza nietypową dla tradycji polskiego prawa pracy formę zatrudnienia, w której funkcjonują trzy podmioty powiązane ze sobą w szczególny sposób. Podmiotami związanymi z pracą tymczasową są: agencja pracy tymczasowej, pracownik tymczasowy oraz pracodawca użytkownik. Szczegółne powiązanie przejawia się po pierwsze w tym, że pomimo występowania trzech podmiotów, zawierane są tylko dwie umowy – pomiędzy agencją pracy tymczasowej i pracodawcą użytkownikiem oraz pomiędzy agencją pracy tymczasowej a pracownikiem tymczasowym. Ponadto funkcjonowanie tej specyficznej

triady przełamuje dotychczas panującą regułę, że pracownik przy wykonywaniu pracy podporządkowany jest tylko swojemu pracodawcy. Spróbuję przybliżyć wzajemne zobowiązania i relacje uczestników pracy tymczasowej.

AGENCJA PRACY TYMCZASOWEJ – PRACOWNIK TYMCZASOWY

Podstawą prawną dla funkcjonowania agencji pracy tymczasowej są Ustawa z dnia 20 kwietnia 2004 r. o promocji zatrudnienia i instytucjach rynku pracy oraz wspomniana już Ustawa o zatrudnieniu pracowników tymczasowych. Według pierwszej, agencję cechuje działalność polegająca na zatrudnianiu pracowników tymczasowych i kierowaniu tych

pracowników oraz osób niebędących pracownikami do wykonywania pracy tymczasowej, na rzecz i pod kierownictwem pracodawcy użytkownika, na zasadach określonych w przepisach o zatrudnianiu pracowników tymczasowych. Działalność agencji pracy tymczasowej polega najpierw na rekrutacji i selekcji potencjalnych pracowników, a następnie, gdy wpływa zgłoszenie od pracodawcy użytkownika zamierzającego pozyskać pracownika o określonych kwalifikacjach, zawarciu z nim umowy i skierowaniu do pracy u pracodawcy użytkownika. Art. 7 Ustawy stanowi, że agencja pracy tymczasowej zatrudnia pracowników tymczasowych, na podstawie umowy o pracę na czas określony lub umowy o pracę na czas wykonania określonej pracy.

Ustawa przewiduje jednak możliwość kierowania do pracy tymczasowej, osób niebędących pracownikami agencji pracy tymczasowej na podstawie umowy prawa cywilnego (np. umowy zlecenia, umowy o dzieło). Strony nie mają przy tym pełnej swobody co do wyboru rodzaju zawieranej umowy. Jeżeli zatrudnienie odbywa się w warunkach wykazujących cechy stosunku pracy (zgodnie z art. 22 par. 1 Kodeksu pracy), to jest to zatrudnienie na podstawie stosunku pracy, bez względu na nazwę zawartej przez strony umowy. Sąd Najwyższy w uchwale z dnia 12 grudnia 2011 r. orzekł, że jeżeli praca tymczasowa odbywa się w warunkach charakterystycznych dla stosunku pracy, to również zatrudnienie osoby skierowanej do pracy tymczasowej na podstawie umowy prawa cywilnego, może być uznane za zatrudnienie na podstawie stosunku pracy. Trzeba jednak uwzględnić, że nie chodzi o typowy stosunek pracy, lecz stosunek pracy z umowy o pracę tymczasową. Dlatego bardzo ważną przesłanką przy dokonaniu oceny, jakiego rodzaju umowę agencja pracy tymczasowej powinna zawrzeć z pracownikiem tymczasowym, jest informacja od pracodawcy użytkownika co do warunków przyszłego zatrudnienia, przede wszystkim dotycząca rodzaju pracy, jaką pracownik ten będzie wykonywał. Jeżeli wykonywanie zadań na rzecz pracodawcy użytkownika będzie przebiegać w warunkach typowo pracowniczych, agencja powinna zawrzeć z pracownikiem tymczasowym umowę o pracę. Nad prawidłowością wyboru rodzaju umowy czuwa Państwowa Inspekcja Pracy, która może wystąpić do sądu o ustalenie stosunku pracy między agencją a osobą wykonującą pracę. W świetle art. 189 Kodeksu postępowania cywilnego takie powództwo przysługuje także osobie, która jest przeświadczona, że świadczy pracę w ramach stosunku pracy, a jest kierowana do niej przez agencję na podstawie umowy cywilnoprawnej.

Agencja pracy tymczasowej, zawierając umowę o pracę z pracownikiem tymczasowym, staje się jego pracodawcą. To ona jako podmiot zatrudniający zawiera i rozwiązuje umowę z pracownikiem, wypłaca mu wynagrodzenie, realizuje zobowiązania urlopowe, wydaje świadectwo pracy, odprowadza składki i podatki. Umowa o pracę pomiędzy tymi stronami zawarta jest głównie po to, aby agencja pracy tymczasowej mogła skierować pracownika tymczasowego do pracy u pracodawcy użytkownika. Daje temu wyraz art. 2 pkt 1 Ustawy, który stanowi, że pracownik tymczasowy, to pracownik zatrudniony przez agencję pracy tymczasowej wyłącznie w celu wykonywania pracy tymczasowej, na rzecz i pod kierownictwem pracodawcy użytkownika. Pracownik tymczasowy formalnie jest zatem pracownikiem agencji, ale fizycznie świadczy pracę na rzecz pracodawcy użytkownika. Co ważne, pracuje pod nadzorem i kierownictwem pracodawcy użytkownika, a to – jak już wspominałam – stanowi swojego rodzaju wyłom w historii polskiego prawa pracy o podporządkowaniu przy świadczeniu pracy tylko swojemu pracodawcy. Pracodawca użytkownik w sensie prawnym nie jest pracodawcą, choć pozyskuje pracownika, który świadczy pracę na jego rzecz i pod jego kierownictwem. Wiąże się to także z pewnymi obowiązkami i konsekwencjami po jego stronie, o czym będzie mowa w dalszej części.

Jak wspominałam powyżej, Ustawa dopuszcza w art. 1 oraz art. 26 możliwość zawierania przez agencję pracy tymczasowej z osobą kierowaną do pracy także umów cywilnoprawnych. Takie rozwiązanie jest możliwe tylko w sytuacji, kiedy praca nie nosi znamion stosunku pracy zgodnie z art. 22 Kodeksu pracy. Agencja zawiera umowę cywilnoprawną, gdy uzasadniają to warunki zatrudnienia u pracodawcy użytkownika, czyli gdy jest to właściwe z uwagi na treść i sposób realizacji warunków zatrudnienia i wynikających z nich obowiązków. W takim przypadku osoba kierowana do pracy nie posiada statusu pracownika, a co za tym idzie, nie może korzystać z przywilejów i przepisów ochronnych prawa pracy. Wobec osób kierowanych do pracy na podstawie umowy cywilnoprawnej, stosuje się odpowiednio przepisy mówiące o zakazie kierowania pracowników tymczasowych do określonych prac, obowiązku uzgodnienia na piśmie z pracodawcą użytkownikiem podstawowych kwestii dotyczących pracy tymczasowej (szerzej o tym poniżej) oraz obowiązku informowania organizacji związkowej o zamiarze powierzenia pracy tymczasowej pracownikowi tymczasowemu. W odniesieniu do tych kwestii Ustawa jasno nakazuje stosowanie przepisów dotyczących zasad zatrudniania pracowników tymczasowych. Można więc uznać,

że w pozostałych kwestiach umowy te podlegają przepisom prawa cywilnego, w którym co do zasady występuje równość stron stosunku prawnego, a strony mogą dobrowolnie kształtować ich treść. Dodatkową ochronę ustawodawca przewidział dla osób w wieku 16-18 lat będących uczniami, a skierowanych do pracy tymczasowej na podstawie umów cywilnoprawnych. Do tej kategorii osób stosuje się odpowiednio przepisy Kodeksu pracy dotyczące zatrudniania młodocianych.

AGENCJA PRACY TYMCZASOWEJ – PRACODAWCA UŻYTKOWNIK

Agencja pracy tymczasowej zawiera umowę o pracę z pracownikiem tymczasowym wtedy, gdy wpływa do niej zgłoszenie pracodawcy użytkownika, zamierzającego pozyskać pracownika o określonych kwalifikacjach. Jeżeli agencja dysponuje kandydatem o poszukiwanym profilu, ma obowiązek zawrzeć z pracodawcą użytkownikiem umowę na piśmie, w której określone są warunki przyszłego zatrudnienia pracownika tymczasowego. Art. 9.1 Ustawy stanowi, że w celu zawarcia umowy o pracę między agencją pracy tymczasowej a pracownikiem tymczasowym pracodawca użytkownik uzgadnia z tą agencją na piśmie:

- rodzaj pracy, która ma być powierzona pracownikowi tymczasowemu;
- wymagania kwalifikacyjne konieczne do wykonywania pracy, która ma być powierzona pracownikowi tymczasowemu;
- przewidywany okres wykonywania pracy tymczasowej;
- wymiar czasu pracy pracownika tymczasowego;
- miejsce wykonywania pracy tymczasowej.

Bardzo ważne jest, aby pracodawca użytkownik przekazał rzetelne informacje co do warunków przyszłego zatrudnienia pracownika tymczasowego. Po pierwsze mają one pomóc wyselekcjonować odpowiedniego kandydata, po drugie determinują rodzaj i treść przyszłej umowy zawartej przez agencję z pracownikiem tymczasowym. Dodatkowo pracodawca użytkownik informuje agencję pracy tymczasowej na piśmie o wynagrodzeniu za pracę, która ma być powierzona pracownikowi tymczasowemu, określonym w przepisach o wynagrodzeniu obowiązujących u pracodawcy użytkownika. Jest to istotne, ponieważ warunki płacowe obowiązujące u pracodawcy użytkownika stanowią podstawę do prawidłowego wyliczenia wynagrodzenia za pracę, wskazanego w umowie o pracę zawieranej między agencją a pracownikiem tymczasowym.

Pracodawca użytkownik zobligowany jest także do poinformowania agencji o warunkach wykonywania



pracy tymczasowej, w zakresie dotyczącym bezpieczeństwa i higieny pracy. Do obowiązków pracodawcy użytkownika w tym zakresie Ustawa zalicza: dostarczenie pracownikowi tymczasowemu odzieży i obuwia roboczego oraz środków ochrony indywidualnej, zapewnienie napojów i posiłków profilaktycznych, przeprowadzenie szkolenia w zakresie bezpieczeństwa i higieny pracy, ustalenie okoliczności i przyczyny wypadku przy pracy, przepro-

na pracodawcy użytkownika cięży ustawowy obowiązek zapewnienia pracownikowi tymczasowemu bezpiecznych i higienicznych warunków pracy w miejscu wyznaczonym do wykonywania pracy. Natomiast na agencji pracy tymczasowej nie spoczywają jedynie obowiązki, którymi pracodawca użytkownik jest obciążony z mocy przepisów prawa lub z mocy zawartej z agencją umowy. Zgodnie z art. 25 Ustawy, w zakresie w niej nieure-

wyposażenie stanowiska pracy), dostarczyć odzież i obuwie robocze, zapewnić napoje i posiłki profilaktyczne, przeprowadzić szkolenie w zakresie BHP, ustalić okoliczności i przyczyny wypadku przy pracy i przeprowadzić ocenę ryzyka zawodowego. Pracodawca użytkownik zobowiązany jest także prowadzić ewidencję czasu pracy pracownika i traktować go, nie mniej korzystnie w zakresie warunków pracy i innych warunków zatrudnienia, niż pracowników zatrudnionych na takim samym lub podobnym stanowisku pracy. W razie naruszenia przez pracodawcę użytkownika zasady równego traktowania, w zakresie warunków pracy, pracownikowi tymczasowemu przysługuje prawo dochodzenia odszkodowania od agencji pracy tymczasowej, w wysokości określonej w przepisach Kodeksu pracy, dotyczących odszkodowania należącego pracownikowi od pracodawcy, z tytułu naruszenia zasady równego traktowania pracowników w zatrudnieniu. Agencja pracy tymczasowej jako formalny pracodawca jest adresem przedmiotowych roszczeń. Ma ona jednak prawo dochodzenia od pracodawcy użytkownika, zwrotu równowartości odszkodowania wypłaconego pracownikowi tymczasowemu.

Obowiązki pracownika tymczasowego w zasadzie nie różnią się od obowiązków innych pracowników, zatrudnionych u pracodawcy. Ma sumiennie wykonywać swoją pracę, stosować się do poleceń przełożonych, przestrzegać przepisów oraz zasad bezpieczeństwa i higieny pracy, czasu pracy oraz regulaminu pracy ustalonego w zakładzie pracodawcy użytkownika.

KTO ODPOWIADA ZA SZKODĘ WYRZĄDZONĄ PRZEZ PRACOWNIKA TYMCZASOWEGO?

Zgodnie z art. 19 Ustawy agencja pracy tymczasowej, jest obowiązana do naprawienia szkody wyrządzonej pracodawcy użytkownikowi przez pracownika tymczasowego przy wykonywaniu pracy tymczasowej. Dzieje się to na zasadach i w granicach obowiązujących pracownika, zgodnie z przepisami o odpowiedzialności materialnej pracowników. Oznacza to, że odpowiedzialność agencji oparta jest na przepisach Kodeksu pracy, co stanowi szczególne postanowienie wyłączające w tym zakresie dochodzenie przez pracodawcę użytkownika od agencji odszkodowania na zasadach przewidzianych w Kodeksie cywilnym, mimo że między nimi została zawarta umowa o charakterze cywilnoprawnym. Można uznać, że odpowiedzialność agencji względem pracodawcy użytkownika jest analogiczna do odpowiedzialności pracownika nietymczasowego, a regulują ją przepisy art. 114-122 Kodeksu pracy. Aby zatem agencja w ogóle odpowiadała za szkodę wyrządzoną przez pracownika tymczasowego, muszą



zaistnieć przesłanki, które warunkują odpowiedzialność materialną zwykłego pracownika. Składają się na nie:

- niewykonanie lub nienależyte wykonanie obowiązków pracowniczych;
- wina po stronie pracownika tymczasowego;
- powstanie szkody w majątku pracodawcy użytkownika;
- adekwatny związek przyczynowy pomiędzy działaniem pracownika a wyrządzoną szkodą.

Istotna jest tutaj kwestia winy pracownika tymczasowego (wina umyślna i nieumyślna), która warunkuje granice odpowiedzialności. Jeżeli pracownik tymczasowy przy wykonywaniu powierzonych mu pracy spowoduje szkodę nieumyślnie – np. na skutek niedbalstwa, lekkomyślnego obchodzenia się z powierzonym mu urządzeniem uszkadza je – to zobowiązanie do naprawienia takiej szkody jest agencją pracy tymczasowej. Odpowiedzialność agencji ogranicza się do rzeczywistej straty pracodawcy użytkownika i jest limitowana do kwoty trzymiesięcznego wynagrodzenia pracownika przysługującego mu w dniu wyrządzenia szkody. Ograniczenie odpowiedzialności do faktycznego uszczerbku majątkowego pracodawcy użytkownika oznacza, że odpowiedzialność ta nie obejmuje tzw. utraconych korzyści – np. równowartości niewyprodukowanej partii butelek, które byłyby wyprodukowane, gdyby pracownik

fot.: Dollarphotoclub.com

tymczasowy nie uszkodził obsługiwanego urządzenia. Za szkodę wyrządzoną przez pracownika tymczasowego z winy umyślniej – np. kradzież pakowanych przez niego części samochodowych – także odpowiada agencja, jednak już do pełnej wysokości poniesionej szkody. Przez naprawienie szkody w pełnej wysokości, odmiennie niż w przypadku winy nieumyślniej, należy rozumieć obowiązek naprawienia rzeczywistej straty poniesionej przez pracodawcę użytkownika, jak również zrekompensowanie mu utraconych korzyści.

Po naprawieniu przez agencję szkody przysługuje jej roszczenie regresowe w stosunku do pracownika tymczasowego o zwrot równowartości odszkodowania, które zostało wypłacone pracodawcy użytkownikowi. Należy pamiętać, że ciężar dowodu spoczywa tutaj na pracodawcy użytkownika, który jest obowiązany wykazać okoliczności uzasadniające odpowiedzialność pracownika tymczasowego oraz wysokość powstałej szkody. Powinien on określić, na czym polegało naruszenie obowiązków pracowniczych, oraz udowodnić, że było ono zawinione (przez niedbalstwo, lekkomyślność, niezachowanie należytej staranności).

Pracownik tymczasowy podczas wykonywania obowiązków pracowniczych może również wyrządzić szkodę osobie trzeciej (innej niż pracodawca użytkownik)

– np. podwykonawcy pracodawcy użytkownika. Ponieważ Ustawa nakazuje w kwestiach w niej nieuregulowanych stosować odpowiednio przepisy prawa pracy dotyczące pracodawcy i pracownika, należy przyjąć, że w takim przypadku agencja pracy tymczasowej, zgodnie z art. 120 Kodeksu pracy, będzie także odpowiadać za szkodę wyrządzoną osobie trzeciej. Warunkiem jest, aby szkoda powstała przy wykonywaniu obowiązków pracowniczych. Zatem, jeżeli podczas wyładowywania towaru dostarczonego do zakładu pracodawcy użytkownika pracownik tymczasowy uszkodzi pojazd należący do osoby trzeciej, odpowiedzialność za taką szkodę spoczywa na agencji pracy tymczasowej, czyli jego pracodawcy. Agencja pracy tymczasowej odpowiada za szkodę w pełnej wysokości, odpowiada bowiem wobec osoby trzeciej na zasadach ogólnych Kodeksu cywilnego. Po naprawieniu przez agencję szkody przysługuje jej roszczenie regresowe do pracownika tymczasowego na warunkach analogicznych, jak za szkodę wyrządzoną bezpośrednio pracodawcy użytkownikowi. Należy przy tym pamiętać, że agencja pracy tymczasowej ponosi odpowiedzialność wyłącznie za szkody powstałe przy wykonywaniu pracy tymczasowej. Jeżeli pracownik tymczasowy, przechodząc obok zakładu pracy po godzinach pracy, wybije umyślnie szybę, za taką szkodę będzie on odpowiadał samodzielnie na podstawie



To pracodawca użytkownik musi zapewnić pracownikowi tymczasowemu bezpieczne i higieniczne warunki pracy.

wadzenie oceny ryzyka zawodowego oraz informowanie o tym ryzyku. Obowiązków tych nie można przenieść na agencję pracy tymczasowej. Prawo nakłada je na pracodawcę użytkownika i to on będzie ponosił odpowiedzialność za należyte wywiązanie się z nich.

Dodatkowo pracodawca użytkownik i agencja pracy tymczasowej powinni, dowolnie, poprzez zawarcie umowy o charakterze cywilnoprawnym, ustalić:

- zakres informacji dotyczący przebiegu pracy tymczasowej, które wpływają na wysokość wynagrodzenia za pracę pracownika tymczasowego, oraz sposób i termin przekazywania tych informacji agencji pracy tymczasowej w celu prawidłowego obliczania wynagrodzenia za pracę tego pracownika (np. praca w godzinach nadliczbowych albo w nocy);
- zakres przejęcia przez pracodawcę użytkownika obowiązków pracodawcy dotyczących bezpieczeństwa i higieny pracy innych niż wskazane powyżej;
- zakres przejęcia przez pracodawcę użytkownika obowiązku pracodawcy dotyczącego wypłacania należności na pokrycie kosztów związanych z podróżą służbową.

Przepisy nie przesądzają, jakie inne niż wynikające z Ustawy obowiązki pracodawcy z dziedziny BHP, mogą być przejęte przez pracodawcę użytkownika (może to być np. obowiązek kierowania pracownika na profilaktyczne badania lekarskie, utworzenia służby BHP, sposób i tryb powołania zespołu powypadkowego). Agencja pracy tymczasowej i pracodawca użytkownik w zawieranej przez siebie umowie, decydują ostatecznie, które obowiązki pracodawcy z tego obszaru, stosownie do możliwości i potrzeb, będą realizowane przez każdą z nich. Jednak niezależnie od tego

gwarantowanym, prawa i obowiązki pracodawcy użytkownika i agencji pracy tymczasowej określa zawarta między nimi umowa. Jej treść ma zatem istotne znaczenie, bo reguluje zasady współpracy, podział obowiązków dotyczących pracownika tymczasowego oraz najważniejsze kwestie dotyczące pracy tymczasowej. Wszelkie ustalenia co do warunków zatrudnienia, jakie przyjmą w umowie agencja pracy tymczasowej z pracodawcą użytkownikiem, trzeba przekazać pracownikowi tymczasowemu. Musi on wiedzieć, który z podmiotów jest obciążony w stosunku do niego, określonymi obowiązkami pracodawcy.

PRACODAWCA UŻYTKOWNIK – PRACOWNIK TYMCZASOWY

Art. 2 Ustawy definiuje pracodawcę użytkownika, jako pracodawcę lub podmiot niebędący pracodawcą w rozumieniu Kodeksu pracy, wyznaczający pracownikowi skierowanemu przez agencję pracy tymczasowej zadania i kontrolujący ich wykonanie. Choć przywołana definicja stanowi, że pracownik tymczasowy świadczy pracę, na rzecz i pod kierownictwem pracodawcy użytkownika, żadna umowa ich nie łączy. Pracodawca użytkownik wykonuje obowiązki pracodawcy tylko w takim zakresie, jaki wynika z przepisów prawa oraz z umowy zawartej z agencją pracy tymczasowej. Pracodawca użytkownik korzysta z praw przysługujących pracodawcy, w zakresie niezbędnym do organizowania pracy z udziałem pracownika tymczasowego. Korzysta z praw w zakresie wyznaczania zadań i bieżącego kontrolowania ich realizacji oraz wydawania poleceń, m.in. dotyczących czynności porządkowych, przygotowawczych i wykonawczych. Musi zapewnić pracownikowi tymczasowemu bezpieczne i higieniczne warunki pracy w miejscu wyznaczonym do wykonywania pracy tymczasowej (odpowiednie



przepisów Kodeksu cywilnego. Inaczej może się kształtować kwestia odpowiedzialności za szkodę wyrządzoną przez osobę, niebędącą pracownikiem agencji, skierowaną do pracy tymczasowej. Ponieważ art. 26.2 Ustawy stanowi, że do osób kierowanych na podstawie umów cywilnoprawnych stosuje się odpowiednio artykuły 8, 9 ust. 1 i 23 Ustawy (omówione powyżej), można uznać, że pozostałe regulacje Ustawy nie będą miały zastosowania względem takich osób. A więc także art. 19 stanowi, że odpowiedzialna za szkodę wyrządzoną przez pracownika tymczasowego jest agencja pracy tymczasowej, na zasadach i w granicach odpowiedzialności materialnej pracowników. Ustawa przewiduje, że w kwestiach w niej nieuregulowanych, prawa i obowiązki pracodawcy użytkownika i agencji pracy tymczasowej określa zawarta między nimi umowa. Zatem strony, korzystając ze swobody umów,

mogą dobrowolnie między sobą ustalić kwestię odpowiedzialności za szkodę wyrządzoną przez osobę kierowaną do pracy tymczasowej na podstawie umowy cywilnoprawnej.

KTO ODPOWIADA ZA SZKODĘ PONIESIONĄ PRZEZ PRACOWNIKA TYMCZASOWEGO?

Podczas wykonywania swoich obowiązków pracownik tymczasowy może być narażony na doznanie wszelkiego rodzaju uszczerbku. Nie ulega wątpliwości, że to pracodawca użytkownik musi zapewnić pracownikowi tymczasowemu bezpieczne i higieniczne warunki pracy. Dodatkowo jednym z jego ustawowych obowiązków wobec pracownika tymczasowego jest ustalenie okoliczności i przyczyn wypadku przy pracy. Jeśli zatem na terenie zakładu pracy doszło do wypadku, w którym poszkodowany został pracownik tymczasowy, pracodawca użytkownik zapewnia mu

pomoc i zabezpiecza w odpowiedni sposób miejsce wypadku. Zobowiązany jest powiadomić o wszystkim agencję pracy tymczasowej zatrudniającą pracownika oraz udostępnić miejsce wypadku, niezbędne materiały i informacje zespołowi powypadkowemu ustalającemu okoliczności i przyczyny wypadku. Agencja pracy tymczasowej i pracodawca użytkownik w umowie mogą doprecyzować, kto sporządza protokół powypadkowy i kto informuje o zdarzeniu Państwową Inspekcję Pracy. Ponieważ pracodawca użytkownik nie ma przymiotu pracodawcy pracownika tymczasowego, wypełniając protokół powypadkowy, w miejsce danych pracodawcy powinien wpisać dane agencji pracy tymczasowej, ponieważ to ona w gruncie rzeczy, jest obciążona zdarzeniem wypadkowym. To ona prowadzi rejestr wypadków przy pracy, sporządza statystyczną kartę wypadku oraz na wniosek pracownika tymczasowego, musi skierować

wniosek do Zakładu Ubezpieczeń Społecznych o ustalenie prawa do świadczeń wypadkowych. Te kwestie w praktyce raczej nie budzą wątpliwości.

Ciekawy jest natomiast przypadek, który trafił w drodze skargi kasacyjnej do Sądu Najwyższego. Dotyczył roszczeń pracownika tymczasowego o zadośćuczynienie i inne roszczenia w związku z wypadkiem przy pracy, skierowanych do pracodawcy użytkownika. Poszkodowany (pracownik tymczasowy), podczas wykonywania pracy tymczasowej w zakładzie pracodawcy użytkownika, został uderzony paletą w plecy i doznał w związku z tym stłuczenia żeber oraz kręgosłupa piersiowego. Agencja pracy tymczasowej sporządziła stosowny protokół. Zakład Ubezpieczeń Społecznych ustalił 13-proc. uszczerbek na zdrowiu i wypłacił jednorazowe odszkodowanie w kwocie 8385 zł. Poszkodowany postanowił skierować swoje dodatkowe roszczenia na drogę sądową i w oparciu o Kodeks cywilny, dochodził od pracodawcy użytkownika roszczeń uzupełniających w kwocie 18 000 zł tytułem zadośćuczynienia oraz 1000 zł tytułem odszkodowania za koszty leczenia z ustawowymi odsetkami od dnia wniesienia pozwu. Powództwo zostało wniesione do Sądu Rejonowego – Sądu Pracy. Pozwana spółka (pracodawca użytkownik) wniosła o oddalenie powództwa w całości, podnosząc, że powód (pracownik tymczasowy) był zatrudniony na podstawie umowy o pracę tymczasową, a jego pracodawcą jest agencja pracy tymczasowej, która powinna być adresem przedmiotowych roszczeń. Sąd Rejonowy przychylił się do tego stanowiska i uznał, że pozwana spółka (pracodawca użytkownik) nie posiada legitymacji biernej w tym procesie. Wskazał, że powód dochodził roszczeń cywilnoprawnych w związku z wypadkiem przy pracy od podmiotu, z którym nie łączył go żaden stosunek prawny. Zdaniem sądu legitymację bierną w tym procesie (procesie ze stosunku pracy i przed sądem pracy) posiada wyłącznie pracodawca powoda, czyli agencja pracy tymczasowej.

Powód (pracownik tymczasowy) wniósł apelację do sądu II instancji. Sąd Okręgowy oddalił ją, uznając, że wprawdzie na pracodawcy użytkownika ciążyą określone przepisami obowiązki pracodawcy względem pracownika tymczasowego, ale nie dają one podstaw do przyjęcia, że odpowiedzialność cywilnoprawną w zakresie skutków wypadku przy pracy ponosi pracodawca użytkownik. Zdaniem sądu co prawda art. 14 Ustawy o zatrudnianiu pracowników tymczasowych stanowi, że pracodawca użytkownik wykonuje obowiązki i korzysta z praw przysługujących pracodawcy, ale jedynie w zakresie niezbędnym do organizowania pracy oraz

zabezpieczenia bezpiecznych i higienicznych warunków pracy. Podtrzymał stanowisko Sądu Rejonowego, że to agencja jako pracodawca, ponosi odpowiedzialność odszkodowawczą z tytułu roszczeń uzupełniających.

Sprawa trafiła w formie skargi kasacyjnej do Sądu Najwyższego. Ten w wyroku z dnia 10 kwietnia 2014 r. uwzględnił skargę, a w uzasadnieniu stwierdził, że w sprawie nie rozpoznano jej istoty wskutek błędnego przyjęcia przez sądy obu instancji, że w sprawie o roszczenia uzupełniające pracownika tymczasowego z tytułu wypadku przy pracy pozwanym może być wyłącznie pracodawca, czyli

PRACA TYMCZASOWA A INNE NIETYPOWE FORMY POZYSKIWIANIA PRACOWNIKÓW

Coraz większy udział w polskim rynku pracy zdobywają niestandardowe formy pozyskiwania pracowników. Pracodawcy często myślą instytucje, które świadczą usługi „wynajmowania pracowników”, a istotnych różnic pomiędzy nimi jest bardzo wiele. Po pierwsze należy odróżnić outsourcing pracowniczy i pracę tymczasową. Usługi te funkcjonują w dwóch różnych ramach prawnych. Pracę tymczasową reguluje Ustawa o zatrudnianiu pracowników tymczasowych i co do zasady przepisy Kodeksu pracy, natomiast outsourcing pracowniczy kształtują prze-

Pracodawcy często mylą instytucje, które świadczą usługi „wynajmowania pracowników”, a istotnych różnic pomiędzy nimi jest bardzo wiele.

agencja pracy tymczasowej. Sąd Najwyższy nie podał w wątpliwość faktu, że pracodawcą pracownika tymczasowego jest agencja pracy tymczasowej. Jednak jak stwierdził, sądy obu instancji wywiodły z tego faktu błędny pogląd, że pracownik tymczasowy nie pozostaje z pracodawcą użytkownikiem w żadnym stosunku prawnym, także w aspekcie uzupełniającej odpowiedzialności odszkodowawczej, na podstawie przepisów Kodeksu cywilnego z tytułu następstw wypadku przy pracy. Ponieważ powód (pracownik tymczasowy) konsekwentnie utrzymywał, że dochodzone roszczenia wywodzi z przepisów prawa cywilnego o czynach niedozwolonych (z art. 435 par. 1 k.c.), który to czyn sam w sobie jest źródłem powstania stosunku zobowiązującego, w jakim odpowiedzialność odszkodowawczą ponosi każdy sprawca szkody. Sąd Najwyższy przychylił się do stanowiska, że pracodawca użytkownik na zasadach ogólnych ponosi ryzyko powstania po stronie pracownika szkód spowodowanych przebiegiem procesu pracy, w tym np. szkód spowodowanych ruchem przedsiębiorstwa, co ma znaczenie zwłaszcza w kontekście roszczeń uzupełniających w wypadkach przy pracy. Dodatkowo uznał, że jeżeli pracownik tymczasowy dochodzi od pracodawcy użytkownika, na podstawie przepisów Kodeksu cywilnego o czynach niedozwolonych, roszczeń uzupełniających (zadośćuczynienia i odszkodowania), to jest to sprawa z zakresu prawa pracy i podlega rozpoznaniu przez sąd pracy.

pisy Kodeksu cywilnego i przede wszystkim umowa handlowa zawarta pomiędzy stronami. Firma outsourcingowa jest także formalnym i faktycznym pracodawcą, i to ona ponosi pełną odpowiedzialność za prace wykonywane przez swoich pracowników.

Kierowanie przez agencję pracy tymczasowej osoby niebędącej pracownikiem agencji, do pracy na podstawie umowy cywilnoprawnej także należy odróżnić od typowego outsourcingu pracowniczego. Pierwsza usługa, jak już wspomniałam, podstawę prawną znajduje w Ustawie o zatrudnianiu pracowników tymczasowych. I chociaż można mieć wątpliwości, czy osoba kierowana do pracy na podstawie umowy cywilnoprawnej ma status pracownika tymczasowego, to niewątpliwie jest ona kierowana do pracy w ramach instytucji pracy tymczasowej. A to determinuje związane z nią obostrzenia, np. co do zakazu wykonywania niektórych prac. W outsourcingu pracowniczym nie ma takich obostrzeń: strony dowolnie kształtują swoje prawa i obowiązki oraz wszelkie zasady i warunki współpracy.

Odróżnić należy także działalność agencji pracy tymczasowej od agencji pośrednictwa pracy, która to udziela pomocy osobom w uzyskaniu odpowiedniego zatrudnienia lub innej pracy zarobkowej oraz pracodawcom w pozyskaniu pracowników >>

o poszukiwanych kwalifikacjach zawodowych. W takich przypadkach umowa o pracę zawierana jest z pracodawcą, a nie z agencją pośrednictwa pracy. Natomiast obie te usługi mogą być realizowane przez agencję zatrudnienia, która oprócz pośrednictwa pracy i pracy tymczasowej, może jeszcze świadczyć usługi doradztwa personalnego i poradnictwa zawodowego.

ZALETY ZATRUDNIANIA TYMCZASOWEGO

Institucja pracy tymczasowej cieszy się z roku na rok coraz większą popularnością, wśród dopuszczalnych form zatrudnienia. Do jej rozwoju przyczyniają się trudne warunki prowadzenia działalności gospodarczej, wynikające w znacznej mierze z rosnącej konkurencji. Pracodawcy, szukając oszczędności, dążą do zmniejszenia kosztów pracy i chcą bardziej elastycznie zarządzać zasobami ludzkimi. Dzięki tej formie zatrudnienia, mogą szybko pozyskać potrzebnych pracowników bez przeprowadzania procesu rekrutacji, a co za tym idzie, obniżyć koszty związane z zatrudnianiem kadry.

Korzystanie z pracowników tymczasowych ma swoje plusy w okresach wzrostu działalności przedsiębiorstwa, kiedy to zapotrzebowanie na siłę roboczą wzrasta. Jest dobre także w okresach kryzysu, gdyż terminowy charakter zatrudnienia sprawia, że stosunek pracy rozwiązuje się przez sam upływ czasu.

Korzystanie z usług agencji pracy tymczasowej nie dotyczy wyłącznie wykonywania przez pracowników tymczasowych prostych prac produkcyjnych czy prac w magazynach. Coraz częściej agencje specjalizują się w zatrudnianiu pracowników będących specjalistami w różnych dziedzinach, np. informatyków, księgowych czy grafików komputerowych.

Tylko agencje posiadające aktualny wpis w Krajowym Rejestrze Agencji Zatrudnienia, działają legalnie i mogą świadczyć usługi w zakresie pracy tymczasowej. Przed nawiązaniem współpracy z daną agencją warto sprawdzić, czy jej wpis figuruje we wspomnianym rejestrze. Sama agencja pracy tymczasowej, jako formalny pracodawca pracowników tymczasowych i jako podmiot z mocy prawa odpowiedzialny za szkody przez nich wyrządzone powinna dla zabezpieczenia swoich interesów posiadać ubezpieczenie od odpowiedzialności cywilnej. Jest ono dostępne w ofercie większości ubezpieczycieli w Polsce. Aby dobrać odpowiedni zakres ubezpieczenia, należy przede wszystkim ustalić, jaką działalność chcemy zgłosić do ubezpieczenia. Czy jest to typowa działalność agencji pracy tymczasowej, która zatrudnia pracowników i kieruje ich do

pracy u pracodawcy użytkownika? Czy także kieruje osoby niebędące pracownikami do pracy tymczasowej na podstawie umów cywilnoprawnych, co zgodnie z Ustawą może czynić? Samo posiadanie polisy OC nie będzie jednak wystarczające – ważny jest dobór odpowiednich klauzul rozszerzających ochronę. Trzeba dopilnować, by zakres ubezpieczenia pokrywał szkody powstałe z wypadków przy pracy, szkody w nieruchomościach osób trzecich, szkody w mieniu znajdującym się w pieczy, pod dozorem lub kontrolą ubezpieczonego czy szkody w rzeczach stanowiących przedmiot obróbki lub naprawy. Zakres powinien też obejmować szkody wyrządzone w środkach transportu, podczas prac ładunkowych, a także szkody wyrządzone wskutek rażącego niedbalstwa. W ten sposób to ubezpieczyciel przejmie na siebie obowiązek zaspokojenia roszczeń, a i w uzasadnionych przypadkach pokryje ewentualne koszty postępowania sądowego. Doświadczenia z pracą tymczasową pokazują, że taka forma zatrudnienia jest potrzebna na polskim rynku pracy. Przede wszystkim pozwala na aktywizowanie ludzi do podejmowania pracy i daje możliwość zdobycia doświadczenia zawodowego osobom, które dopiero zaczynają karierę zawodową. Jednocześnie jest to stosunkowo młoda instytucja, która cały czas dynamicznie się zmienia, by odpowiadać na potrzeby rynku. Niestety, nie idą za tym zmiany legislacyjne, a istotne zapisy pozostają niezmienione od lat. Rzadkość nowelizacji i brak rozbudowanej linii orzecniczej sprawiają, że przepisy dotyczące pracy tymczasowej są często nieprecyzyjne i niedopasowane do realiów. Właśnie dlatego, stosując zatrudnienie tymczasowe, należy uważnie oraz precyzyjnie konstruować postanowienia umowne, tak aby w możliwie jak najmniejszym stopniu uniknąć niejasności. ■

BIBLIOGRAFIA

- Ustawa z dnia 9 lipca 2003 r. o zatrudnianiu pracowników tymczasowych, Dz.U. 2003, nr 166, poz. 1608.
- Ustawa z dnia 20 kwietnia 2004 r. o promocji zatrudnienia i instytucjach rynku pracy, Dz.U. 2004, nr 99, poz. 1001.
- Ustawa z dnia 26 czerwca 1974 r. Kodeks pracy, Dz.U. 1974, nr 24, poz. 141.
- Uchwała Sądu Najwyższego z dnia 12 grudnia 2011 r. I UZP 6/11.
- Ustawa z dnia 17 listopada 1964 r. Kodeks postępowania cywilnego, Dz.U. 1964, nr 43, poz. 296.
- Wyrok Sądu Najwyższego z dnia 10 kwietnia 2014 r. Sygn. akt I PK 243/13.
- Ustawa z dnia 23 kwietnia 1964 r. Kodeks cywilny, Dz.U. 1964, nr 16, poz. 93.
- Praca tymczasowa od A do Z, pod red. Małgorzaty Dobrowolskiej, Rzeszów 2007.



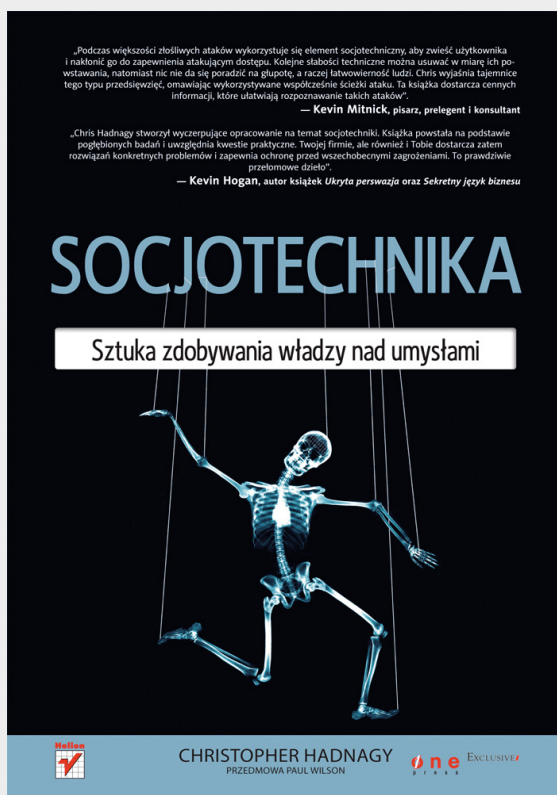
Agata Kowalczyk

Specjalista ds. Ubezpieczeń w Biurze Ubezpieczeń Odpowiedzialności Cywilnej. Absolwentka Wydziału Prawa i Administracji Uniwersytetu Gdańskiego oraz studiów podyplomowych na kierunku ubezpieczenia i rynki kapitałowe na Uniwersytecie Szczecińskim. W Grupie ERGO Hestia od 2008 r.



agata.kowalczyk@ergohestia.pl

KSIĄŻKA



SOCJOTECHNIKA.

Sztuka zdobywania władzy nad umysłami

Ludzki umysł to najmocniejszy z elementów każdego systemu.

Ludzki umysł to najsłabszy z elementów każdego systemu.

Brzmi paradoksalnie? A jednak bez względu na to, jak skomplikowane ustanowisz zabezpieczenia, Twoje przedsięwzięcie może się nie udać właśnie z winy człowieka. Każdy z nas funkcjonuje według pewnych schematów, które można z powodzeniem rozgryźć. A złośliwy socjotechnik o odpowiednich umiejętnościach to przeciwnik, przed którym niemal nie sposób się obronić. Social engineering to nadal silny oręż w rękach biznesmenów, polityków, pseudowróżek, ale również hakerów. Autor bardzo przejrzyście wyjaśnia psychologiczne zasady socjotechniki, jednocześnie dając wskazówki, jak rozpoznać zagrożenie i jak się przed nim bronić. ■

KONFERENCJA

TARGI BEZPIECZEŃSTWA I HIGIENY PRACY SAWO



Pod koniec kwietnia 2016 r. na terenie Międzynarodowych Targów Poznańskich, odbędą się Targi Bezpieczeństwa i Higieny Pracy SAWO. W tym organizowanym co dwa lata wydarzeniu wezmą udział czołowe polskie przedsiębiorstwa oraz uznani w Europie producenci i dystrybutorzy światowych marek. SAWO to największe targi BHP w Europie Środkowo-Wschodniej. W ostatniej edycji uczestniczyło 203 wystawców z 23 krajów. Zakres tematyczny obejmuje takie obszary jak: środki ochrony indywidualnej i zbiorowej, wyposażenie miejsc pracy, ochrona przeciwpożarowa, oznakowanie bezpieczeństwa, sprzęt i środki dla służb ratowniczych oraz pojazdy gaśnicze i specjalne. Nowością najbliższych targów będzie Aleja Ergonomii, w której zostaną pokazane najnowocześniejsze rozwiązania z zakresu ergonomii pracy.

ERGO
HESTIA®



ERGO Hestia drugi raz z rzędu
najlepsza w opinii pracowników
warsztatów samochodowych!