Nr 2/2013 (22)

RISKFOCUS

OBLICZA RYZYKA

TOP SECRET
Wojna psychologiczna o bezpieczeństwo informacji

Płyty warstwowe – jak z nimi żyć?

Spokojnie, to tylko awaria

O bezpieczeństwie flot bez uprzedzeń

ERGO HESTIA®

70%

z pierwszych dziesięciu firm branży energetyka i ciepłownictwo ubezpiecza Ergo Hestia.

wg listy 500 tygodnika Polityka 2012 r.

Ergo Hestia
Jestem pewien

ERGO HESTIA®

Infolinia: **801 107 107**
koszt połączenia wg taryfy operatora

www.ergohestia.pl

Drodzy Czytelnicy!

Lato wprawdzie już za nami, ale okres wyjazdów – wcale nie. Wszak wielu z nas wybiera się na urlop jesienią. Niech więc trwa jak najdłużej czas przyjemności, zwiedzania, fascynujących przygód, wzmożonej aktywności czy słodkiego nicnierobienia. Ale to również czas ryzyka...

Uświadomiłem to sobie podczas tegorocznych wakacji. Dwa dni przed lotem na uroczą śródziemnomorską wyspę dowiedziałem się, że szaleją tam pożary lasów. Władze były zmuszone do ewakuacji mieszkańców i turystów z obszarów zagrożonych. Odetchnąłem z ulgą, gdy okazało się, że tereny objęte pożarem znajdują się w odległości kilkudziesięciu kilometrów od naszej wakacyjnej bazy. Bezpośredniego zagrożenia nie było, więc ruszyliśmy w dobrych nastrojach.

Kolejny problem pojawił się wraz z wysoką gorączką mojej młodszej córeczki. Gdyby nie stosowna polisa i kompetencje lokalnego lekarza, urlop mógłby stać się dla nas prawdziwym koszmarem. Napływające jednocześnie z mediów informacje na temat zamieszek w jednym z krajów arabskich i związanych z nimi kłopotów turystów dodatkowo utwierdziły mnie w przekonaniu, że w czasie wakacji szczególnie należy mieć się na baczności.

Podczas tego, nieco pechowego, wyjazdu dowiedziałem się również, że „Risk Focus" otrzymał wyróżnienie w światowym konkursie Content Marketing Awards wśród publikacji sektora ubezpieczeniowego. Uczciliśmy to lampką... hiszpańskiej cavy. Wierzę, że podzielają Państwo – przynajmniej w części – zdanie jurorów tego prestiżowego konkursu.

Tymczasem zachęcam do uważnej lektury nowego numeru naszego magazynu. Mam nadzieję, że przedstawione tematy z zakresu oceny ryzyka czy rozwiązań ubezpieczeniowych to nie tylko duża dawka wiedzy, ale również inspiracja do dalszej aktywności w biznesie. Oczywiście z zachowaniem wszelkich zasad bezpieczeństwa.

Zbigniew Żyra
Redaktor Naczelny

spis treści
nr 2/2013

Fot.: STU Ergo Hestia SA

Redaktor Naczelny: Zbigniew Żyra
Zespół redakcyjny: Kamil Bara, Hubert Rutkowski, Aleksandra Sosnowska-Serek, Jacek Woronkiewicz

Produkcja: Polish Creative Group
Koordynacja projektu: Angelika Kucińska
Projekt graficzny: Diana Kosiorek
Druk: Drukarnia WL

Adres: ul. Hestii 1, 81-731 Sopot
tel.: +48 58 555 62 27
e-mail: risk.focus@ergohestia.pl
www.ergohestia.pl

1 mld rubli – na taką kwotę oszacowano straty po wybuchu meteoru nad Uralem w okolicach Czelabińska. Zostało uszkodzonych prawie 300 budynków, w tym szpitale i szkoły.

ŚWIAT

WYBUCHOWY AMONIAK

W zakładach chemicznych Stirol w mieście Horliwka w obwodzie donieckim na Ukrainie doszło 6 sierpnia 2013 r. do wybuchu amoniaku. W wyniku eksplozji zginęło sześciu pracowników, a 20 rannych trafiło do szpitala. Wszystko wskazuje na to, że wybuch spowodowała nieostrożność podczas prac remontowych. Według lokalnych władz i kierownictwa firmy zdarzenie nie przyniosło strat w najbliższym sąsiedztwie zakładu. Koncern Stirol należy do Grupy DF Dmytra Firtasza, aktywnej w takich dziedzinach jak: energetyka, przemysł chemiczny, infrastruktura energetyczna i nieruchomości. RF

KOSMICZNY deszcz meteorytów

Telefony komórkowe przestały działać, w autach włączały się alarmy, a w oknach pękały szyby. Prawie 300 budynków zostało uszkodzonych, w tym szpitale, przedszkola, szkoły i obiekty sportowe. W fabryce cynku zawalił się dach i runął fragment muru. Poważnie ucierpiał również budynek Czelabińskiego Uniwersytetu Państwowego. Ponad 1100 osób zostało rannych. Straty sięgnęły 1 mld rubli. Taki jest bilans wybuchu meteoru, do którego doszło nad Uralem w okolicach Czelabińska 15 lutego 2013 r. Zdaniem NASA podczas wybuchu uwolniona została energia 500 kt (kiloton). Dla porównania: Little Boy, bomba atomowa, która zniszczyła Hiroszimę w 1945 r., uwolniła energię 15 kt. Rosyjska Akademia Nauk oceniła, że masa meteoru przed jego wejściem w ziemską atmosferę wynosiła 10 t, a jego średnica 15 m. Meteoryt to pozostałość drobnego skalnego ciała niebieskiego (meteoroidu) przyciągniętego przez znacznie większe ciało niebieskie, która w postaci ciała stałego dociera do jego powierzchni. RF

Z KRAJU

PODPALENIE?

Dwie godziny – tyle trwało gaszenie pożaru, który wybuchł 17 lipca 2013 r. na terenie fabryki Hutmen we Wrocławiu. Ogień pojawił się w dwóch halach magazynowych firmy zajmującej się recyklingiem. Na szczęście strażacy szybko opanowali płomienie, dlatego wstępnie straty oszacowano na poziomie 100 – 200 tys. zł. Prawdopodobnie przyczyną pożaru było podpalenie, na co wskazuje przede wszystkim duża odległość pomiędzy halami, uniemożliwiająca przeniesienie się ognia. A może to po prostu zbieg okoliczności? RF

BACILLUS CEREUS

To nie jest niestety łacińska nazwa egzotycznego motyla, lecz bakterii

chorobotwórczej, która spowodowała zbiorowe zatrucie w Olsztynie i w Dobrym Mieście. Na początku września 2013 r. doszło do zatrucia pacjentów szpitala w Dobrym Mieście oraz pensjonariuszy domu pomocy społecznej w Olsztynie. Firma cateringowa przygotowująca posiłki dla tych instytucji najprawdopodobniej nie zachowała standardów higienicznych. Wskutek spożycia dań zakażonych laseczką woskową (bo taką nazwę nosi owa bakteria) zachorowało prawie 90 osób. Producenci gotowych posiłków kierowanych do tego typu obiektów (szpitale, stołówki w szkołach) powinni zachować wyjątkowe środki ostrożności ze względu na podwyższoną podatność odbiorców dań na zatrucia. Wyższe niż standardowe sumy gwarancyjne w ubezpieczeniu OC działalności gospodarczej są w takich przypadkach wskazane. RF

PRZEMYSŁ

WYCIEK AMONIAKU

– 100 ton zatrutych ryb

Chińskie władze usunęły z 40-kilometrowego odcinka rzeki Fu w środkowych Chinach około 100 t ryb zatrutych przez wyciek amoniaku z zakładów chemicznych Hubei Shuanghuan Science and Technology Stock Co. W próbkach ścieków odprowadzanych przez firmę stężenie amoniaku przekraczało wielokrotnie chińskie normy. – Śnięte ryby wypłynęły na powierzchnię całej rzeki i wyglądały jak śnieg – opowiadał jeden z mieszkańców wioski, której mieszkańcy żyją głównie z rybołówstwa. Gwałtowny rozwój przemysłowy Chin w ostatnich 30 latach, nieegzekwowanie przepisów oraz niewłaściwa kontrola wpływają na degradację środowiska naturalnego. RF

Nowe rozporządzenie W SPRAWIE SIECI GAZOWYCH

5 września 2013 r. weszło w życie nowe rozporządzenie w sprawie warunków technicznych, jakie powinny spełniać sieci gazowe i ich usytuowanie (Dz.U. 2013, poz. 640). Nowe przepisy określają m.in. rodzaje materiałów, z których można budować sieci, a także regulują kwestie kolizji z infrastrukturą podziemną. Rozporządzenie Ministra Gospodarki doprecyzowuje inne istotne wymagania związane z bezpieczeństwem, np. armaturę zaporową i upustową. Do ostatniej poważnej awarii sieci gazowej doszło 30 listopada 2010 r. w Zielonej Górze, gdzie wskutek najprawdopodobniej wadliwie wykonanej modernizacji stacji redukcyjnej gazu w sieci wzrosło jego ciśnienie, gaz zaczął się ulatniać i w końcu eksplodował w kuchenkach gazowych. Zginęła wówczas jedna osoba, doszło do pożarów i zniszczenia wielu mieszkań. Ewakuowano tysiące osób. RF

Ile kosztuje PIĘKNO?

Czy będzie rekordowe zadośćuczynienie za doznaną krzywdę? Trwa proces sądowy przeciwko Pomorskiemu Centrum Traumatologii im. Mikołaja Kopernika w Gdańsku. W sierpniu 2010 r. przeprowadzono w nim zabieg powiększenia piersi szwedzkiej obywatelki. Skutki okazały się dramatyczne dla poszkodowanej, która do dziś pozostaje w śpiączce. Sąd zajął się badaniem przyczyn zaistniałej sytuacji i długa będzie droga do oceny, czy – jak tego oczekują pełnomocnicy poszkodowanej – anestezjolog i personel szpitala popełnili błędy. Odpowiedzialność szpitala według pełnomocnika poszkodowanej wynika z błędów organizacyjnych, zaniedbań personelu medycznego, naruszenia standardów postępowania i procedur medycznych przy udzielaniu świadczeń zdrowotnych. Uwagę zwraca szczególnie kwota żądnego zadośćuczynienia: 6 mln zł! Czy jest możliwe ustalenie rekordowego zadośćuczynienia za doznaną krzywdę? Jaką cenę ma pragnienie piękna? Odpowiedzi na te pytania pozostaną tajemnicą dla samej poszkodowanej. Dla sądu będą trudnym zadaniem do rozwiązania. RF

90 osób

zachorowało po spożyciu dań zakażonych laseczką woskową. Firma cateringowa dostarczająca posiłki do szpitala w Dobrym Mieście i domu pomocy społecznej w Olsztynie nie zachowała standardów higienicznych.

Fot.: Shutterstock

TOP SECRET
Wojna psychologiczna o bezpieczeństwo informacji

KAŻDY Z NAS W JAKIMŚ STOPNIU JEST ŚWIADKIEM EWOLUCJI SPOŁECZEŃSTWA, KTÓRE OBECNIE JEST NAZYWANE SPOŁECZEŃSTWEM INFORMACYJNYM I WYKORZYSTUJE ZAAWANSOWANE TECHNOLOGIE INFORMATYCZNE. **NAJCENNIEJSZYM TOWAREM JEST W NIM INFORMACJA – SPECYFICZNE DOBRO NIEMATERIALNE. SPECYFICZNE, BO CORAZ CZĘŚCIEJ CENIONE WYŻEJ OD DÓBR MATERIALNYCH I, CO ZA TYM IDZIE, PODLEGAJĄCE SZCZEGÓLNEJ OCHRONIE.**

Tekst: **Karolina Andryskowska**

Często spotykamy się ze stwierdzeniem, że człowiek jest najsłabszym ogniwem w łańcuchu elementów wpływających na bezpieczeństwo informacji. Praktycznie każde rozwiązanie techniczne, opracowane przez najlepszych inżynierów, a zapobiegające wyciekowi informacji, może zostać przypadkowo lub celowo ominięte przez człowieka. Hakerzy, by podnieść skuteczność wykorzystywanych przez siebie technologii, stosują różnego rodzaju socjotechniki. Próby włamania do złożonych systemów informatycznych, zaopatrzonych w mechanizmy zabezpieczające, zajmują po prostu zbyt wiele czasu. Człowiek jest zdecydowanie łatwiejszym celem. Wystarczy wykorzystać kilka psychologicznych prawd o jego naturze.

Zazwyczaj wyżej cenimy wygodę niż bezpieczeństwo. Nic więc dziwnego, że jesteśmy dla hakerów i innych internetowych oszustów łakomym kąskiem. Korzystanie z komputera podłączonego do Internetu jest już powszechne zarówno w pracy, jak i w domu. Jednak nie każdy wie, że stałe połączenie z siecią znacząco zwiększa ryzyko infekcji złośliwym oprogramowaniem. Świadomość, że wiąże się to z narażeniem użytkowników oraz ich danych na zagrożenie, jest ciągle bardzo niska, a ewentualne konsekwencje ataku nas nie interesują. Co więcej, często nie dopuszczamy do siebie myśli o tym, że może on być realny. Tymczasem próby włamania się do komputera, szpiegowania czy kradzieży danych lub tożsamości zdarzają się coraz częściej. Mogą się przytrafić każdemu, o ile nie będzie wystarczająco ostrożny.

PRZYZWYCZAJENIE DRUGĄ NATURĄ CZŁOWIEKA

Korzystając z komputerów domowych, zazwyczaj opieramy się na przyzwyczajeniach. Weźmy choćby kwestię działania programów antywirusowych. Wiele zadań przez nie realizowanych jest aktywnych w tle, co oznacza, że są niewidoczne przy standardowym użytkowaniu komputera. Dodatkowo oprogramowanie antywirusowe jest często preinstalowane przez dostawcę sprzętu: kupujemy nowy komputer, który już ma wgrany program antywirusowy. Takie rozwiązanie jest oczywiście wygodne, ale sprzyja pogłębianiu naszej niewiedzy: jeśli niczego samodzielnie nie instalowaliśmy, wydaje nam się, że jesteśmy zwolnieni z obowiązku dbania o to. Wszystkie te aspekty składają się na niezbyt korzystny obraz nas samych jako użytkowników komputerów domowych, nieświadomych własnych działań.

Załóżmy, że mimo wszystkich przeszkód posiedliśmy wiedzę wystarczającą, by jednoznacznie stwierdzić: tak, mam antywirusa. Tymczasem mało kto przy zakupie sprzętu komputerowego zwraca uwagę na to, że oprogramowanie antywirusowe cechuje się ograniczonym okresem użytkowania, np. ma licencję tylko na rok. Zbyt rzadko interesujemy się również tym, czy zabezpieczenia funkcjonują prawidłowo, czy baza wirusów jest aktualna (na szczęście większość programów aktualizuje ją automatycznie), czy licencja na posiadane oprogramowanie jest ważna.

Co ciekawe, okazuje się, że jedną cechę antywirusów zna większość z nas: wiemy, że działanie takiego programu wiąże się z odczuwalnym spowolnieniem komputera. Co więc najczęściej robimy? Wybieramy opcję „odinstaluj" i po kilku minutach możemy odetchnąć z ulgą. Możemy pracować wydajniej...

Większość z nas to szczęśliwi posiadacze komputera z dostępem do Internetu. Jak z niego korzystamy? Sieć daje nam duże poczucie wolności i pozornego bezpieczeństwa. Nie reagujemy na powiadomienia o możliwym zainfekowaniu komputera, akceptując tym samym obecność wirusów i stając się zagrożeniem dla innych użytkowników. Najbardziej jednak szkodzimy sami sobie. Programy antywirusowe (czy ogólnie zabezpieczenia komputera) bowiem nie są naszą jedyną piętą achillesową. W badaniu przeprowadzonym przez Kaspersky Lab, jednego z głównych producentów rozwiązań bezpieczeństwa na świecie, luki w zabezpieczeniach oprogramowania stanowią ogromne zagrożenie dla bezpieczeństwa komputerów. Dzieje się tak dlatego, że stają się głównym narzędziem włamań wykorzystywanym do kradzieży danych użytkowników czy przeprowadzania ataków. „Analiza danych pochodzących od ponad 11 mln użytkowników ujawniła występowanie ponad 132 mln luk w zabezpieczeniach wykrytych w różnych programach – średnio 12 luk na użytkownika", podaje raport firmy Kaspersky Lab[1]. Wynika z niego jednoznacznie, że powinniśmy bezwzględnie pamiętać o regularnym aktualizowaniu systemu operacyjnego oraz posiadanego oprogramowania (szczególnie jeśli chodzi o oprogramowanie typu Java, Adobe Flash oraz Adobe Reader).

SZEŚĆ GRZECHÓW GŁÓWNYCH

Załóżmy, że nasz komputer ma aktualny program antywirusowy oraz bieżące wersje pozostałego oprogramowania. Czy możemy myśleć, że jesteśmy bezwzględnie bezpieczni? Kilka grzechów popełniamy najczęściej.

[1] *Raport dostępny na stronie www.kaspersky.pl.*

Zbyt rzadko interesujemy się tym, czy zabezpieczenia funkcjonują prawidłowo,

czy baza wirusów jest aktualna (na szczęście większość programów aktualizuje ją automatycznie), czy licencja na posiadane oprogramowanie jest ważna.

>>

Fot.: Shutterstock

Nie uważamy na hasła. Często przechowujemy je w plikach dostępnych dla innych użytkowników. Co więcej, pliki te nazywamy „hasła", żebyśmy my, a także inni wiedzieli, jaka zawartość znajduje się w środku. Mało tego, przenosimy te pliki na inne komputery lub pamięci przenośne.

Korzystamy z niezabezpieczonych sesji (http://). Wypełniając formularze danymi lub logując się do usług typu bankowość elektroniczna czy zakupy internetowe, powinniśmy wybierać szyfrowaną wersję protokołu – https://. Korzystamy z niezabezpieczonych sieci Wi-Fi.

Używając obcego sprzętu komputerowego, pozostawiamy niewylogowane sesje, nie czyścimy historii przeglądania, a nawet wyrażamy zgodę na zapamiętywanie haseł!

Wykorzystujemy sprzęt firmowy – komputery, smartfony – do celów prywatnych (np. zakupów przez Internet).
Jesteśmy zbyt ufni. Beztrosko otwieramy załączniki wiadomości, nie zwracając uwagi na jej treść. Akceptujemy zdecydowanie zbyt dużo komunikatów oraz reklam dystrybuowanych w formie wyskakujących okienek. Jak ognia unikajmy klikania „OK/Akceptuję" w ostrzeżeniach na stronach, które oferują usuwanie złośliwego oprogramowania lub których pochodzenie jest wątpliwe.

Powyższe „grzechy" pokazują, jak ważne dla naszego bezpieczeństwa są podstawowe, proste czynności wykonywane praktycznie codziennie. Nasze działania związane z korzystaniem z Internetu opierają się zazwyczaj na przyzwyczajeniach, rzadko kiedy bierzemy pod uwagę to, że kwestia bezpieczeństwa (komputera czy sieci) zmienia się bardzo dynamicznie. Pozostajemy więc w miejscu, nie pogłębiając wiedzy na temat bezpieczeństwa. Tym samym nie uświadamiamy sobie nowych zagrożeń. Na szczęście zadbanie o bezpieczeństwo nie jest tak trudne, jak mogłoby się wydawać.

NIE TAKI DIABEŁ STRASZNY

Większość naszych działań związanych z bezpieczeństwem informacji sprowadza się do ochrony sprzętu przed zainfekowaniem szkodliwym oprogramowaniem. Okazuje się, że podjęte przez nas starania mogą być nieefektywne, gdyż – jak podają specjaliści – najczęściej instalacji szkodliwego oprogramowania dokonuje sam użytkownik. Własnoręcznie! Wystarczy do tego jedno kliknięcie.

Pracując na komputerze, czy to firmowym, czy prywatnym, chcemy uczynić jego użytkowanie przyjemniejszym, więc personalizujemy niektóre jego ustawienia

Naszą nieświadomość ochoczo przenosimy z realiów prywatnych w struktury firmowe. Wychodzimy często z założenia, że zabezpieczenia firmowej sieci i komputerów są na tyle zaawansowane, że możemy sobie pozwolić na brak czujności.

– tapetę, wygaszacz ekranu, wszystko, co się da. Okazuje się jednak, że „wśród oprogramowania skrywającego w sobie malware [szkodliwe oprogramowanie] na czoło wysuwają się wygaszacze ekranów. (...) Podobnie prawdopodobnym jego źródłem mogą być darmowe gry i inne samowykonywalne (z rozszerzeniem .exe) aplikacje"[2]. Musimy więc nauczyć się przykładać większą wagę do tego, co pobieramy z Internetu, a przede wszystkim postarajmy się nie korzystać z odnośników, których popularność jest zastanawiająco niska.

Korzystając z dobrodziejstw Internetu, powinniśmy stosować zasadę ograniczonego zaufania i przełożyć ją bezpośrednio na zasadę nieklikania. Najczęściej będzie ona miała zastosowanie w przypadku wyskakujących okienek, które tylko czyhają na okazję, by zatruć nam życie. Ileż to razy mieliśmy ochotę przez nie udusić własny komputer, klikając kilkadziesiąt razy przycisk „Anuluj", który nie powodował żadnej reakcji? Ile razy zrezygnowani, dla świętego spokoju, wybraliśmy jednak przycisk „OK", by tylko zakończyć tę gehennę? Ile razy po takim kliknięciu otrzymaliśmy komunikat o zagrożeniu infekcją wirusem, który od razu proponował nam antidotum? Dla ilu z nas owo antidotum okazało się prawdziwą trucizną? Otóż jednym ze sposobów na wyskakujące okienka i komunikaty jest nieużywanie przycisków w nich zawartych. Znacznie lepiej jest kliknąć prawym przyciskiem myszy wyskakującą reklamę/komunikat na pasku zadań i z menu wybrać opcję „Zamknij". Prawda, że proste?

GRANICE ZAUFANIA

Pisałam wcześniej o korzystaniu z niezabezpieczonych sesji oraz o tym, że powinniśmy wybierać szyfrowane wersje połączeń – to brzmi bardzo prosto. Jednak jak je zidentyfikować? Tutaj z pomocą przychodzi nam protokół SSL, który jest jednym z narzędzi wykorzystywanych do skutecznej ochrony naszych danych przed ich przechwyceniem. Zazwyczaj wymiana danych z i do serwera odbywa się poprzez przesyłanie przez sieć otwartego tekstu, który względnie łatwo przechwycić (szczególnie w sieci lokalnej). Gdy serwer używa protokołu SSL do komunikacji z przeglądarką, informacja w obie strony (między serwerem WWW i przeglądarką) jest transportowana w sposób zaszyfrowany. Adresy internetowe zabezpieczone przy użyciu protokołu SSL zaczynają się od https://, a nie http://, często też możemy spotkać się z określeniem protokołu SSL jako HTTPS. Certyfikat SSL natomiast jest odpowiednikiem dokumentu tożsamości. Certyfikaty są wydawane przez niezależne i zaufane urzędy – Certification Authorities (CA). Łącząc się z serwerem WWW, sprawdzajmy nie tylko ważność certyfikatu, ale również informacje zawarte w certyfikacie (np. prawidłową nazwę właściciela).

[2] *J. Viega, Mity bezpieczeństwa IT. Czy na pewno masz się czego bać? Helion, Gliwice 2010, s. 26.*

Może się zdarzyć, że strona nie będzie miała szyfrowanego połączenia, co wtedy? Warto zwrócić na to uwagę właściciela strony. Kwestia bezpieczeństwa danych klientów jest coraz poważniej traktowana przez firmy (również ze względów wizerunkowych), więc możemy liczyć na to, że uwagi zostaną przyjęte i poprawki szybko będą widoczne na stronie.

Internet stał się nieodłączną częścią naszego życia. Chcąc nie chcąc, musimy mu trochę zaufać. Granica bezpieczeństwa jest jednak cienka, a zbytnia ufność może szybko uczynić z nas ofiary kradzieży tożsamości. Kradzież ta oznacza wykorzystanie wizerunku albo innych danych osobowych w celu wyrządzenia szkody majątkowej lub osobistej. To rodzaj oszustwa, którego skutkiem jest przechwycenie danych osobistych, tj. hasła, nazwy użytkowników, danych bankowych czy numerów kart kredytowych. W odniesieniu do środowiska internetowego takie działania są nazywane phishingiem. W tym procederze najczęściej wykorzystywane są wiadomości e-mail lub fałszywe strony internetowe stworzone właśnie po to, aby wykradać dane osobiste. Oszuści posługują się milionami fałszywych wiadomości e-mail zawierających linki do spreparowanych stron internetowych. Strony te do złudzenia przypominają oficjalne wiadomości od różnych organizacji i instytucji zaufania publicznego, takich jak banki lub towarzystwa ubezpieczeniowe. Stworzone są jednak po to, by wymusić na nas (przy wykorzystaniu socjotechnik) podanie danych osobistych. Cyberprzestępcy wykorzystują te informacje przy popełnianiu kolejnych przestępstw, takich jak kradzież pieniędzy z konta, otwarcie nowego konta w naszym imieniu czy zdobycie poufnych dokumentów przy wykorzystaniu naszej tożsamości.

CZUJNOŚĆ PRZEDE WSZYSTKIM

RSA, dział zabezpieczeń firmy EMC (największy na świecie dostawca rozwiązań w zakresie bezpieczeństwa oraz zarządzania ryzykiem), w najnowszym raporcie „Online Fraud Report" prezentuje trendy w atakach typu phishing. Wskazują one jednoznacznie, że ataki te są niezmiennie ogromnym zagrożeniem dla firm i użytkowników. W poprzednim roku RSA zidentyfikował średnio 37 tys. ataków phishingowych miesięcznie[3]. Jak zatem rozpoznać fałszywe wiadomości e-mail? Poniżej kilka znaków ostrzegawczych[4], które pojawiają się w otrzymywanych wiadomościach i powinny obudzić naszą czujność:

- alarmujące wiadomości i groźby zamknięcia konta;
- obietnice korzyści majątkowych (konkretnych kwot) w zamian za mały wysiłek lub bez wysiłku;
- oferty, które wydają się zbyt korzystne, by mogły być prawdziwe;
- prośby o darowizny dla organizacji charytatywnej, np. po klęsce żywiołowej, o której mówiono w środkach masowego przekazu;
- błędy gramatyczne i ortograficzne.

Dobrą wiadomością jest niewątpliwie to, że nie jesteśmy osamotnieni w walce z oszustami, a pomoc napływa do nas z wielu stron. Wykwalifikowani pracownicy organów ścigania podążają za trendami przestępczymi i są wyposażani w wyspecjalizowane narzędzia, by iść nam z pomocą w razie problemów. Kodeks karny również został przystosowany do nowych realiów i w myśl art. 190a § 2: „osoba dopuszczająca się phishingu podlega karze pozbawienia wolności do lat 3 (jeżeli następstwem tego czynu, jest targnięcie się osoby pokrzywdzonej na własne życie, sprawca podlega karze pozbawienia wolności od roku do lat 10)".

Podejmuje się również wiele inicjatyw mających na celu poszerzenie wiedzy użytkowników, firm działających w branży bezpieczeństwa IT. Pod koniec 2012 r. specjaliści z CERT Polska (specjalny zespół powołany do reagowania na zdarzenia naruszające bezpieczeństwo w sieci Internet) zaangażowali się w redakcję przeznaczonych dla polskich użytkowników materiałów na tematy związane m.in. z kradzieżą tożsamości.

Na stronie internetowej[5] CERT-u dostępny jest test złożony z kilkunastu pytań dotyczących sytuacji z życia wziętych, w których narażeni jesteśmy na kradzież tożsamości. Opracowany materiał edukuje osobę poddającą się badaniu szczególnie przez sekcję „Czytaj i ucz się", w której znalazło się wiele informacji dotyczących badanej problematyki. Odpowiadając sumiennie na zadane pytania, uzyskamy procentowy wynik wskazujący, w jakim stopniu nasze codzienne działania chronią nas przed kradzieżą tożsamości.

Opis sześciu grzechów głównych we wspomnianym tekście nie tylko wytyka nam niedoskonałości i beztroskę postępowania, ale też wskazuje proste rozwiązania podnoszące poziom bezpieczeństwa naszych rutynowych działań. Zerwanie z dotychczasowymi przyzwyczajeniami jednak nie jest łatwe, wymaga nakładu pracy i dyscypliny. Dodatkowo utrzymanie poziomu bezpieczeństwa będzie wymagało od nas choćby minimalnego zainteresowania tematem ochrony danych w przyszłości. Cel jest jednak wart zaangażowania – chodzi w końcu o bezpieczeństwo naszych danych.

Musimy mieć świadomość, że błędy popełniane przez nas podczas pracy w domu przekładają się często na firmowe środowisko IT. Naszą nieświadomość ochoczo przenosimy z realiów prywatnych w struktury firmowe. Wychodzimy często z założenia, że zabezpieczenia firmowej sieci i komputerów są na tyle zaawansowane, że możemy sobie pozwolić na brak czujności. Nic bardziej mylnego. W końcu w firmowych bazach przechowywane są również nasze dane. Czy teraz, kiedy właśnie sobie to uświadomiliśmy, nadal chcemy postępować pochopnie?

Sektor bezpieczeństwa zmienia się bardzo intensywnie. Bezustannie doskonalone są normy i protokoły bezpieczeństwa. Dostępność nowoczesnych zabezpieczeń oprogramowania i sprzętu sprawia, że przestępcom jest coraz trudniej pisać skuteczne szkodliwe oprogramowanie, przejmować kontrolę nad systemami komputerowymi i wykradać dane. Rozwój trwa nieprzerwanie, jedyną stałą pojawiającą się w łańcuchu bezpieczeństwa jest człowiek. Warto więc zadbać o to, byśmy nie pozostawali dłużej najsłabszym ogniwem. RF

Karolina Andryskowska
Pracuje w Biurze Ryzyka i Bezpieczeństwa Informacji, w Dziale Systemowego Zarządzania Ryzykiem, zajmuje się bezpieczeństwem informacji, absolwentka Akademii Marynarki Wojennej, w Grupie Ergo Hestia od 2008 r.

karolina.andryskowska@ergohestia.pl

[3] *Raport jest dostępny na stronie: www.emc.com/collateral/fraud-report/rsa-online-fraud-report-012013.pdf.*

[4] *Przykłady tzw. znaków ostrzegawczych zaczerpnięte ze strony www.microsoft.com*

[5] *http://www.cert.pl/news/6193.*

Fot.: Shutterstock, STU Ergo Hestia SA

PŁYTY WARSTWOWE
– jak z nimi żyć?

W CZERWCU 2009 R. POŻAR NIEMAL CAŁKOWICIE ZNISZCZYŁ KOMPLEKS PRODUKCYJNO-MAGAZYNOWY DUŻEGO KRAJOWEGO ZAKŁADU Z BRANŻY SPOŻYWCZEJ. SUMA SZKÓD SIĘGAJĄCA WEDŁUG RÓŻNYCH PUBLIKACJI PRASOWYCH 100 MLN ZŁ NIE ZASKOCZYŁA ZBYTNIO RYNKU UBEZPIECZENIOWEGO. W KOŃCU NOTOWANO JUŻ WYŻSZE STRATY. JEDNAK ZDARZENIE NISZCZĄCE PRAWIE 100 PROC. **OBIEKTU, I TO W ZNACZNEJ CZĘŚCI WYKONANEGO Z PŁYT WARSTWOWYCH, POZOSTAWIŁO TRWAŁY ŚLAD W PODEJŚCIU UBEZPIECZYCIELI DO WYKONANYCH Z NICH BUDYNKÓW. CHOROBA ZWANA „ALERGIĄ NA PŁYTY WARSTWOWE" OGARNĘŁA NIEMAL CAŁY KRAJOWY RYNEK UBEZPIECZENIOWY.**

Tekst: **Krzysztof Kowalczyk**

Niektórzy oceniający ryzyko, słysząc podczas wizyty, że gdzieś występuje płyta warstwowa, z miejsca dyskwalifikowali – w ramach technicznej oceny ryzyka – całe kompleksy obiektów. Za tym sposobem myślenia podążali underwriterzy będący dodatkowo pod presją osiągania jak najlepszych wyników technicznych, i to akurat po tąpnięciu na światowych rynkach finansowych spowodowanym upadkiem banku Lehman Brothers we wrześniu 2008 r.

W ciągu ostatnich 10-15 lat przeobraził się krajobraz naszego kraju, co wszyscy możemy zauważyć, jednak nie wszyscy widzą, że w nowych obiektach przemysłowych technologia murowana i żelbetowa została zastąpiona konstrukcją stalową ze ścianami wykonanymi właśnie z płyt warstwowych.

ZALETY: WARSTWA PO WARSTWIE

Konieczne jest w tym miejscu wyjaśnienie, jak jest zbudowana płyta warstwowa, która w swoim czasie wywołała tyle zamieszania na krajowym rynku ubezpieczeniowym. W bardzo dużym uproszczeniu: płyta składa z dwóch warstw blachy (stalowej lub – rzadziej – aluminiowej), pomiędzy którymi znajduje się rdzeń z pianki poliuretanowej, styropianu lub wełny mineralnej o grubości od kilku do kilkunastu centymetrów. Podstawowymi zaletami stosowania płyt warstwowych są stosunkowo niska cena i łatwy montaż, a ten ostatni ściśle wiąże się z czasem budowy obiektu. Przykładowo: w przypadku gdy mamy dwa obiekty jednokondygnacyjne (a takie najczęściej są obecnie stawiane do celów produkcyjnych i magazynowych) o tych samych wymiarach, czas budowy obiektu o konstrukcji żelbetowej lub murowanej ze ścianami w tej samej technologii jest co najmniej trzykrotnie dłuższy niż czas postawienia budynku o konstrukcji stalowej ze ścianami z płyt warstwowych. Także cena pierwszego może być dwa i więcej razy wyższa niż obiektu drugiego typu. W rzeczywistości wysokiej konkurencji na rynku powyższe zalety są nie do przecenienia.

CIEKAWOSTKA: LOTNICZE POCZĄTKI

Płyty warstwowe zaczęto niemal powszechnie stosować w obiektach przemysłowo-magazynowych mniej więcej w połowie lat 90. ubiegłego wieku. Obecnie z dużą odpowiedzialnością można stwierdzić, że ponad 90 proc. zakładów produkcyjnych i hal magazynowych powstaje w tzw. technologii płyty warstwowej. Oznacza to, że zarówno ściany zewnętrzne, jak i wewnętrzne budowanych obiektów są wykonane z płyt warstwowych, a szkielet budynku ma stalową konstrukcję.

Historia płyt sięga początków XIX w. Według źródeł internetowych pierwsza płyta warstwowa została wytworzona w 1820 r. Bezpośrednio przed II wojną światową brytyjska firma lotnicza De Havilland wykorzystała płyty warstwowe w konstrukcji samolotów bojowych. Ich okładziny stanowiła sklejka, a rdzeń był wykonany z balsy – lekkiego drewna o dużej giętkości i wyporności. Przełomem w wykorzystywaniu różnych materiałów jako rdzenia w płytach warstwowych było odkrycie i opatentowanie w 1937 r. przez Otto Bayera reakcji chemicznej umożliwiającej uzyskiwanie spienionych poliuretanów oraz wynalezienie styropianu przez Friedricha Rudolfa Stastny'ego w 1949 r.

Współczesna płyta warstwowa pojawiła się w 1960 r., kiedy firma Alside unowocześniła produkcję płyt z wykorzystaniem okładzin drewnianych na tyle, że stały się one konkurencyjne cenowo. W tym samym czasie rozpoczęto produkcję płyt warstwowych z wykorzystaniem okładzin metalowych.

A jak to było w Polsce? W Obornikach Wielkopolskich (stąd powszechne nazywanie płyt warstwowych „płytami obornickimi") w latach 1974-1975 uruchomiono pierwsze w kraju linie produkcyjne do wytwarzania płyt typu PW8/B. Obecnie w kraju istnieje kilku znaczących producentów płyt warstwowych.

RDZEŃ PROBLEMU: ZAGROŻENIE PRZECIWPOŻAROWE

Jak już wspomniano, płyta warstwowa składa się z dwóch warstw zewnętrznych i wypełnienia, tzw. rdzenia. Wierzchnie warstwy mogą być wykonane z różnych materiałów (stal, aluminium, miedź, płyta wiórowa, okładzina tynkowa), zaś znajdujący się pomiędzy nimi rdzeń jest zwykle wykonany z pianki poliuratanowej (PIR lub PUR), styropianu lub wełny mineralnej.

Najczęściej wykorzystywane są płyty, których warstwy zewnętrzne stanowi blacha stalowa. Ze względu na materiał, z jakiego wykonany jest ich rdzeń, płyty te są znakomitym elementem izolacyjnym. Stąd ich niemalże powszechne zastosowanie w przemyśle spożywczym (z pewnymi wyjątkami dotyczącymi płyt z wykorzystaniem jako rdzenia wełny mineralnej). Nie mniej istotnym aspektem przemawiającym za upowszechnieniem stosowania płyt warstwowych, wpływającym także na łatwość montażu, jest niewielki ciężar przypadajacy na jednostkę powierzchni.

IZOLACYJNOŚĆ

	Gęstość [kg/m^3]	Współczynnik przewodności cieplnej [W/mK]
Poliuretan (PUR/PIR)	≥35	≥0,025
Styropian (EPS/XPS)	≥15	≥0,035
Wełna mineralna	≥100	≥0,040

Źródło: materiały własne

Mimo wszystkich pozytywnych cech płyty – szczególnie z wypełnieniem z tworzyw sztucznych: pianki poliuretanowej i styropianu – stwarzają, w określonych warunkach, ogromne zagrożenie pożarem. Pianki PUR/PIR podczas pożaru zwęglają się, nie ulegając stopieniu i teoretycznie nie rozprzestrzeniając ognia. Z kolei styropian nie dość, że się pali, to jeszcze w temperaturze 90°C dodatkowo topi się, a spadające zapalone krople mogą rozprzestrzeniać pożar.

Różnica pomiędzy piankami poliuretanowymi PIR (poliizocjanowymi) a zwykłymi piankami PUR jest taka, że pierwsze zawierają więcej izocjanów niż te drugie, co znacząco poprawia ich właściwości ogniowe, tzn. podczas pożaru wydzielają znacznie mniejsze ilości dymu oraz na powierzchni pianki tworzy się zwęglina chroniąca jej wnętrze przed dalszym oddziaływaniem temperatury. Zawsze jednak należy pamiętać, że pianki poliuretanowe oraz styropian są tworzywami sztucznymi pochodzenia organicznego i będą ulegały rozkładowi termicznemu podczas pożaru z wydzieleniem znacznych ilości dymu i ciepła już w temperaturze 300-400°C. Kolejnym istotnym mankamentem płyt warstwowych (ze względu na ich cechy pożarowe) jest niska trwałość stalowych warstw zewnętrznych. Stal staje się plastyczna już w temperaturze 500-600°C, w temperaturze powyżej 1000°C zaczyna topnieć, co ma niewątliwy wpływ na zachowanie się rdzenia płyty (wykonanego z tworzyw sztucznych).

Niezwykle ważnym elementem, ze wglądu na możliwość przenikania ciepła do wnętrza płyty, a mającym wpływ na zachowanie się obiektów zbudowanych z płyt warstwowych w czasie pożaru jest sposób połączenia ich ze sobą. Wyróżnia się dwa typy połączenia: na styk z taśmą uszczelniającą i nakładkowo-zakładkowy z taśmą uszczelniającą. Przy zastosowaniu drugiego typu połączenia płomienie nie mają szans na bezpośrednie i szybkie dotarcie do rdzenia płyty. Dlatego stosowanie systemu zakładkowo-nakładkowego w łączeniu płyt jest dużo lepszym rozwiązaniem (z punktu widzenia bezpieczeństwa pożarowego) niż połączenie płyt w systemie na styk.

PRAKTYKA: PALĄCA POTRZEBA ZASAD BEZPIECZEŃSTWA

Gaszenie pożaru obiektu zbudowanego z płyt warstwowych jest często nieskuteczne, ponieważ nie można dotrzeć z wodą do zabudowanego rdzenia płyty. Dlatego strażacy muszą najpierw oderwać blachę znajdującą się na zewnątrz płyty, aby następnie dostać się do rdzenia i rozpocząć gaszenie zarzewia pożaru. Nie dość, że jest to niezmiernie trudne i czasochłonne, to jeszcze mało skuteczne. Dlatego gaszenie tego typu obiektów sprowadza się bardziej do zapobiegania nierozprzestrzenianiu się ognia na sąsiadujące obiekty niż działań stricte gaśniczych. Najistotniejsze jest zatem bezwzględne przestrzeganie zasad bezpieczeństwa pożarowego podczas budowania i użytkowania obiektów z płyt warstwowych.

Statystyki pokazują, że pożary obiektów zbudowanych z płyt warstwowych, prowadzące do dużych strat materialnych, powstawały w efekcie zapalenia się rdzenia płyt, co było spowodowane przede wszystkim niewłaściwym zabezpieczeniem przejść kabli energetycznych przez ściany. Bezpośrednie opieranie się kabli o ostre krawędzie blachy przy przechodzeniu przez ściany z płyt warstwowych jest najczęściej spotykanym błędem instalacyjnym. W wyniku naturalnego procesu zużywania się po pewnym czasie użytkowania instalacji w obiekcie następuje uszkodzenie izolacji kabla, dochodzi do zwarcia przewodu z warstwą zewnętrzną (blachą) płyty i zanim zadziałają zabezpieczenia elektryczne, wydziela się ilość energii wystarczająca do zapalenia się rdzenia płyty.

Praktycznym rozwiązaniem, poprawiającym bezpieczeństwo pożarowe, jest prowadzenie >>

Fot.: Shutterstock

przewodów energetycznych przez ściany z płyt warstwowych w metalowych rurkach ochronnych, które skuteczne zabezpieczają kable przed uszkodzeniem o ostre krawędzie blach oraz dodatkowo odcinają od bezpośredniego kontaktu z rdzeniem płyty.

90 proc.

– aż taki odsetek zakładów produkcyjnych i hal magazynowych powstaje w technologii tzw. płyty warstwowej.

Ponadto należy unikać sytuacji, w których ładowanie akumulatorów wózków transportowych (wykorzystywanych powszechnie zarówno w halach produkcyjnych, jak i magazynowych) odbywa się bezpośrednio przy ścianach z płyt warstwowych. Konieczne jest oddzielenie ściany z płyty warstwowej od stanowisk ładowania dodatkową ścianą o odporności ogniowej co najmniej 60 min. Należy także zauważyć, że składowanie wszelkich materiałów wykonanych z drewna lub tworzyw sztucznych, ze względu na znaczne ilości energii emitowanej podczas spalania, powinno się odbywać w odległości co najmniej 10 m od ścian wykonanych z płyty warstwowej.

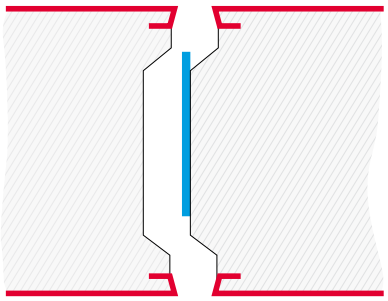
Kolejnym istotnym elementem podnoszącym bezpieczeństwo stosowania płyt warstwowych jest badanie rezystancji izolacji (co najmniej raz w roku) wszystkich instalacji elektrycznych położonych na płytach i przez nie przechodzących. Niedopuszczalne jest pozostawianie odkrytego rdzenia płyty po wykonaniu w obiektach zbudowanych z płyt warstwowych jakichkolwiek prac związanych z montażem nowych instalacji, aranżowaniem pomieszczeń itp. Wszelkie miejsca, gdzie rdzeń płyty jest widoczny, należy każdorazowo osłonić odpowiednią obróbką blacharską.
Płyty warstwowe, tak jak wiele elementów budowlanych, posiadają właściwą im odporność ogniową.
Płyty z rdzeniem z pianki poliuretanowej (PUR i PIR), styropianu oraz wełny mineralnej o określonej grubości rdzenia mają cechy oddzieleń przeciwpożarowych, ustalone na podstawie badań wykonywanych przez certyfikowane jednostki badawcze. Jednak warunki laboratoryjne wielokrotnie odbiegają od dynamiki rzeczywistego pożaru, co w konsekwencji ma wpływ na faktyczną weryfikację odporności ogniowej. Dotychczas w kraju nie odnotowano przypadku, aby płyta warstwowa w warunkach faktycznego pożaru zachowała się tak samo skutecznie jak ściana oddzielenia przeciwpożarowego wykonana z cegły lub żelbetonu o podobnym czasie odporności ogniowej.

Dotychczasowe statystyki, a także podane powyżej przykłady wskazują, że w razie pożaru obiektu wykonanego z płyt warstwowych opartego na stalowej konstrukcji zawsze dojdzie do całkowitego jego zniszczenia. Stąd tak bardzo istotne jest przestrzeganie reguł wpisanych w kompleksową koncepcję ochrony przeciwpożarowej. Płyty warstwowe, ze względu na swoje zalety związane przede wszystkim z ceną oraz łatwym i szybkim montażem, jeszcze długo będą tworzyć przemysłowy krajobraz. Trzeba więc nauczyć się z nimi żyć i konsekwentnie egzekwować podstawowe zasady bezpieczeństwa związane z ich stosowaniem. RF

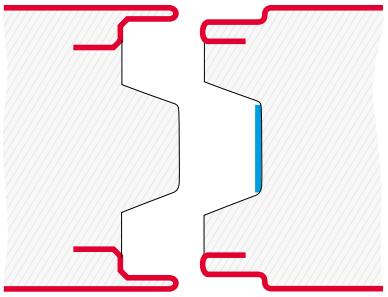
Źródła:

- *Sandwich elements as room – closing wall roof components. VdS 2006.*
- *J. Sawicki, Płyty warstwowe w sztywnych okładzinach metalowych, Dom Wydawniczy „Medium", Warszawa 2010.*
- *Wiedza i doświadczenie pracowników Hestia Loss Control Sp z o.o.*

RODZAJE POŁĄCZEŃ PŁYT WARSTWOWYCH



połączenie w systemie na styk



połączenie w systemie nakładkowo-zakładkowym

Krzysztof Kowalczyk
Hestia Loss Control, specjalista ds. oceny ryzyka, zajmuje się zagadnieniami ryzyka ogniowego i utraty zysku, inżynier, absolwent Szkoły Głównej Służby Pożarniczej w Warszawie, w Grupie Ergo Hestia od 1994 r.

krzysztof.kowalczyk@ergohestia.pl

80%

firm notowanych na Giełdzie Papierów Wartościowych ubezpiecza Ergo Hestia.

WIG 20, 2013 r.

Ergo Hestia
Jestem pewien

Infolinia: **801 107 107**
koszt połączenia wg taryfy operatora

www.ergohestia.pl

ERGO HESTIA®

Spokojnie to tylko AWARIA

PESYMISTYCZNE PROGNOZY GOSPODARCZE PO 2008 R. NIE SPRZYJAJĄ BEZPIECZNEMU PROWADZENIU DZIAŁALNOŚCI PRZEDSIĘBIORSTWA. OPRÓCZ NIEKORZYSTNEJ KONIUNKTURY PRZEDSIĘBIORCY SĄ NARAŻENI TAKŻE NA SKUTKI ZDARZEŃ LOSOWYCH, KTÓRE NIE TYLKO POWODUJĄ WYMIERNE STRATY W MIENIU, ALE PRZEDE WSZYSTKIM MOGĄ WYWOŁAĆ ZAKŁÓCENIA LUB PRZERWĘ W DZIAŁALNOŚCI, A TYM SAMYM PRZYNIEŚĆ STRATĘ W UZYSKIWANYM DOCHODZIE.

Tekst: **Krzysztof Dąbrowski**

W niektórych przypadkach po klasycznym i najczęściej wybieranym ubezpieczeniu BI (Business Interruption) warto pomyśleć o uszczelnieniu ochrony przedsiębiorstwa przez rozszerzenie o MLOP (Machinery Loss Of Profit), czyli ubezpieczenie utraty zysku w wyniku awarii maszyn.

PRZYKŁAD 1

Styczeń 2011 r. Firma Odważni sp. z o.o., produkująca części samochodowe, otrzymuje dotację unijną na zakup maszyn i urządzeń. W związku z tym powiększa swój park maszynowy o nowe, innowacyjne maszyny o wartości 6 mln euro. Mając wysoką wydajność i duże moce produkcyjne, firma podpisuje wielomilionowe kontrakty z jednym z największych producentów samochodów, który stał się głównym odbiorcą części (80 proc. produkcji). Prezes firmy postanowił przetransferować ryzyko awarii maszyn do ubezpieczyciela. Pośrednik przekazał ofertę towarzystwa ubezpieczeń... i zaczęła się kalkulacja oraz liczenie oszczędności:

- składka za ubezpieczenie maszyn od ognia : 20 tys. zł,
- składka na ubezpieczenie maszyn od awarii: 48 tys. zł.
- składka na ubezpieczenie od strat związanych z awariami maszyn: 30 tys. zł.

Prezes po naradzie z dyrektorem finansowym oraz brygadzistą postanowił: „Ubezpieczenie od awarii jest nam niepotrzebne, przecież mamy nowe urządzenia na gwarancji". Po przeliczeniu kosztów stwierdził: „Zatrudnię pracownika do utrzymania maszyn i jeszcze połowa ceny ubezpieczenia pozostanie w kasie firmy".

Jak postanowił, tak zrobił. Zatrudnił pana Czesława na stanowisku specjalisty ds. utrzymania maszyn (dawniej konserwatora maszyn) za jedyne 3,5 tys. zł brutto. Prawie wszyscy zadowoleni. Firma funkcjonuje rewelacyjnie, główny odbiorca zadowolony z jakości i dotrzymywanych terminów, zwiększyła się liczba części zamawianych w firmie Odważni sp. z o.o. Zamówień przybywa i praca musi się odbywać na trzy zmiany siedem dni w tygodniu.

Do czasu. Nadchodzi sądny dzień, 1 maja 2011 r. Prezes będący na urlopie otrzymuje informację o przestoju w zakładzie. Dzwoni do pana Czesława i słyszy: „Panie prezesie, spokojnie, to tylko awaria, poradzimy sobie w jednej chwili". Spokojny pan prezes kontynuuje wypoczynek. Jest pewny, że produkcja lada moment zostanie wznowiona. Następnego dnia w dalszym ciągu kluczowa maszyna nie pracuje. Pan Czesław nie jest już taki opanowany. Właściciel postanawia wezwać serwis zewnętrzny producenta

Fot.: Shutterstock

maszyny. Pada diagnoza – na pierwszy rzut oka pozytywna: uszkodzenie. Jednak po dłuższej analizie okazuje się, że nie dotyczy ono odpowiedzialności gwarancyjnej producenta, przyczyną szkody była błędna obsługa pracownika firmy. Wymiana uszkodzonego elementu kosztuje jedyne 10 tys. zł, ale trzeba jeszcze na nowo przeprogramować maszynę. Czas oczekiwania na wyspecjalizowaną ekipę oraz samo programowanie zajmie około dwóch miesięcy.

W wyniku przestoju oraz braku niezbędnych środków do transferu produkcji (tymczasowe przeniesienie produkcji do konkurencji to koszt około 700 tys. zł) firma straciła głównego odbiorcę. Następnie przyszła utrata zaufania rynku, a co za tym idzie – zerwanie kolejnych kontraktów i ogłoszenie upadłości firmy.

PRZYKŁAD 2

Rok 2008. Elektrociepłownia Lawa SA przed sezonem grzewczym oddała do eksploatacji blok gazowo-parowy. Biznesplan przygotowany w sezonie letnim 2007 r. uwzględniał koszt montażu przez wyspecjalizowaną ekipę oraz koszt ubezpieczenia bloku od awarii. Po ciężkim dla branży ciepłowniczej sezonie zimowym 2007/2008 zarząd spółki postanowił szukać oszczędności i podjął decyzję o rezygnacji z ubezpieczenia (padło stwierdzenie: „Wystarczająca będzie ochrona bloku od ognia"). Postanowiono również, że część prac montażowych wykonają pracownicy firmy: „Przecież mamy wyspecjalizowanych techników".

Obszar działania przedsiębiorstwa obejmował jedno z kilkudziesięcio-tysięcznych miast. Elektrociepłownia miała monopol lokalny. Firma opierała swoją działalność na kilku blokach gazowo-parowych. Zakupiony blok gazowo-parowy miał być kluczowy dla przedsiębiorstwa w sezonie 2008/2009. Zakładano, że będzie generował 50 proc. energii wytwarzanej przez firmę.

Pracownicy przystępują do montażu bloku. Zakończenie prac montażowych następuje w październiku. Próby i testy przebiegają pomyślnie: można zacząć eksploatację. 28 grudnia podczas nocnej zmiany nowy blok ulega awarii i przestaje pracować. Początkowo wydaje się, że to tylko krótkotrwałe zakłócenie w pracy. Po przybyciu serwisu okazuje się, że uszkodzenie jest poważne. Na szczęście naprawa nie jest zbyt kosztowna, jednak długotrwała. Remont wirnika należy przeprowadzić u producenta.

Nieobecność na rynku

przez okres potrzebny na odtworzenie majątku trwałego może spowodować, że dotychczasowi klienci przedsiębiorstwa dotkniętego szkodą znajdą nowych partnerów handlowych.

Trudność nie polegała jedynie na długim czasie naprawy. Skomplikowane było ustalenie przyczyny awarii. Należało jednoznacznie określić, po czyjej stronie leży odpowiedzialność. Badania wykazały, że konieczne jest wykonanie naprawy wirnika u producenta. Czas naprawy u producenta – 1,5 miesiąca. Remont wirnika musiał być wstrzymany do momentu ustalenia przyczyny zdarzenia. Prace zmierzające do ustalenia przyczyny zdarzenia trwały 45 dni. Ostatni miesiąc to montaż elementów oraz testy i rozruch turbiny po naprawie. Od powstania szkody do wznowienia działalności minęło pięć miesięcy.

Elektrociepłownia została zmuszona do ograniczenia produkcji. Przychody przedsiębiorstwa pochodziły ze sprzedaży energii elektrycznej i cieplnej. W ujęciu rocznym przychody oscylowały w okolicach 100 mln zł. Straty (utrata zysku) wyniosły około 23 mln zł. Dodatkowo nie pokryto kosztów zakupu energii na własne potrzeby, pracy biegłych rewidentów. Łącznie wszystkie straty związane ze szkodą mieściły się w granicach 40 proc. rocznego obrotu przedsiębiorstwa. Brak ubezpieczenia utraty zysku wskutek awarii maszyny poskutkował zachwianiem płynności finansowej.

A MOGŁO BYĆ INACZEJ...

Wystarczyła jedna decyzja o przekazaniu ryzyka utraty zysku ubezpieczycielowi i sytuacja firmy wyglądałaby zgoła odmiennie.

Pierwsze przypadki ubezpieczania szkód następczych i zysku utraconego datuje się na przełom XVIII i XIX w., kiedy to rynek brytyjski zaczął oferować taki produkt. W ślad za rynkiem >>

brytyjskim podążył rynek niemiecki, proponując od 1817 r. ubezpieczenie utraty czynszu jako dodatek do ubezpieczeń ogniowych nieruchomości będących przedmiotem najmu. Rok 1821 przyniósł znaną do dziś metodę kalkulacji odszkodowania opartą na okresie przerwy w działalności liczonym w dniach. Rok 1899 z kolei uważa się za datę powstania dominującego dziś modelu ubezpieczenia opartego na przychodach jako kluczowym parametrze. Wiek XX i rewolucja technologiczna przyniosły wprowadzenie ubezpieczeń utraty zysku kroczących w ślad za awarią maszyn. W 1910 r. niemiecki organ nadzoru zatwierdził taki produkt finansowy i dopuścił go do sprzedaży (W. Meier, M. Kuhn, A. Simone, E. Sormani, G. Galey, Business Interruption Insurance, Swiss Re, Zürich 2004).

Na podstawie przedstawionych przykładów firmy Odważni sp. z o.o. oraz Lawa SA można zauważyć, jak dotkliwa bywa przerwa w działalności wywołana zdarzeniem losowym. Przyczyn tego jest wiele.

Na znaczeniu zyskują posiadane kontakty handlowe, kompetencje kluczowych pracowników czy kultura organizacyjna. Klasyczne ubezpieczenie mienia nie chroni tych elementów. W wyniku niesamowitej globalizacji nasiliła się konkurencja. Nieobecność na rynku przez okres potrzebny na odtworzenie majątku trwałego może spowodować, że dotychczasowi klienci przedsiębiorstwa dotkniętego szkodą znajdą nowych partnerów handlowych. Ponadto outsourcing i specjalizacja produkcji zwiększają liczbę i rozległość geograficzną powiązań biznesowych. W rezultacie zdarzenie losowe u dostawcy może powodować trudności z zachowaniem ciągłości działalności w całym łańcuchu dostaw.

Rynek ubezpieczeniowy oferuje produkty zabezpieczające powyższe działania. Jednym z nich jest ubezpieczenie MLOP. Przedmiotem ubezpieczenia jest ubezpieczeniowy zysk brutto[1], który zostałby przez ubezpieczającego osiągnięty, gdyba szkoda nie zaistniała. Za utratę zysku uważa się poniesioną przez ubezpieczającego w okresie odszkodowawczym[1] stratę finansową, bezpośrednio wynikającą ze spadku obrotu i wzrostu kosztów wytwarzania, powstałą wskutek zakłóceń lub przerwy w działalności, będących następstwem zdarzenia. Sumę ubezpieczenia mogą kształtować podatki, kredyty, energia elektryczna, a także koszty zastąpienia uszkodzonej maszyny lub przeniesienia produkcji do innej lokalizacji.

KONKLUZJA

Podsumowując powyższe przemyślenia, należy zauważyć, że ubezpieczenie MLOP jest godnym rozważenia elementem programu ubezpieczenia przedsiębiorstwa produkcyjnego. Decydując się na to ubezpieczenie, należy uwzględnić koszty i korzyści płynące z takiego działania. Koszt to oczywiście składka, ale również dodatkowe rozwiązania techniczne i organizacyjne, których wdrożenia wymaga ubezpieczyciel. Płatność składki w okresie normalnej działalności przedsiębiorstwa bowiem jest relatywnie niewielkim ciężarem. Korzyść z uzyskania odszkodowania w razie zaistnienia określonego umową zdarzenia może być natomiast ogromna – szczególnie gdy jego wypłata decyduje o przetrwaniu przedsiębiorstwa.

Czy nie warto więc kupić spokoju w przypadku wystąpienia awarii? RF

1. Zagadnienia omówione szerzej w artykułach: To BI or not to BI? „Risk Focus" 2013, nr 1; Transfer ryzyka utraty zysku, „Risk Focus" 2007, nr 4.

Krzysztof Dąbrowski
specjalista ds. ubezpieczeń, zajmuje się zagadnieniami majątkowymi i technicznmi oraz budowlano-montażowymi, absolwent Wydziału Mechanicznego Politechniki Gdańskiej, pracuje w Biurze Ubezpieczeń Podmiotów Gospodarczych. W Grupie Ergo Hestia od 2004 r.

krzysztof.dabrowski@ergohestia.pl

Fot.: STU Ergo Hestia SA

87%

firm budowlanych notowanych na Giełdzie Papierów Wartościowych ubezpiecza Ergo Hestia.

WIG-BUDOW., 2013 r.

Ergo Hestia
Jestem pewien

ERGO HESTIA®

Infolinia: **801 107 107**
koszt połączenia wg taryfy operatora

www.ergohestia.pl

SZANSA
jedna na milion

TRAF, PRZYPADEK, PRAWDOPODOBIEŃSTWO – TYCH SŁÓW UŻYWAMY, OPISUJĄC MOŻLIWOŚĆ ZAISTNIENIA JAKIEGOŚ ZDARZENIA. NAJCZĘSTSZYM PRZYKŁADEM SYTUACJI, W KTÓREJ WIĘKSZOŚĆ OSÓB CHCIAŁABY UCZESTNICZYĆ, JEST TRAFIENIE SZÓSTKI W LOSOWANIU LOTTO. I CHOĆ SZANSA TAKA WYNOSI 1 DO 13 983 816, RZESZE LUDZI KUPUJĄ LOSY. SKORO TAK ŁATWO CZASAMI JEST NAM UWIERZYĆ W TO, ŻE SPOTKA NAS COŚ POZYTYWNEGO, DLACZEGO NIE JESTEŚMY W STANIE PRZYJĄĆ, ŻE STWIERDZENIE: „MNIE NA PEWNO COŚ TAKIEGO SIĘ NIE PRZYTRAFI" JEST W SPORYM STOPNIU WYŁĄCZNIE MYŚLENIEM ŻYCZENIOWYM?

Tekst: **Rafał Perczak**

Powyższe dotyczy zarówno życia ludzi, jak i funkcjonowania firm. Niekorzystnych zdarzeń mogących wpłynąć na prowadzoną przez przedsiębiorców działalność gospodarczą jest bez liku. Od problemów z otrzymywaniem płatności za świadczone usługi, przez zmiany prawa, po kryzysy gospodarcze oraz przeróżne zdarzenia losowe. W niniejszym artykule zajmiemy się tymi ostatnimi, związanymi z odpowiedzialnością cywilną z tytułu prowadzonej działalności gospodarczej. Warto w jej kontekście przyjrzeć się przykładom pewnych zdarzeń.

CZŁOWIEK POTYKA SIĘ NIE O GÓRY, A O KRETOWISKA

Autorstwo tej prostej maksymy przypisuje się powszechnie Konfucjuszowi. Jak większość tego typu złotych myśli, jest ona próbą ujarzmienia przynajmniej w części mechaniki otaczającego nas świata. Aforyzm ten mówi po prostu: choć to duże rzeczy zwracają na siebie uwagę, drobiazgi potrafią doprowadzić do upadku.

NIE MIERZ INNYCH SWOJĄ MIARĄ

Pierwszy przykład dotyczy firmy świadczącej usługi geodezyjne. Zawarła ona umowę na wytyczenie granic działki pod budynek zabudowy szeregowej wraz z jego posadowieniem w terenie. Prace wykonano w ciągu jednego dnia, budowę rozpoczęto. Gdy roboty już trwały i kończono konstrukcję parteru, kierownik budowy z pewnym zaskoczeniem stwierdził, że budynek stoi w niewłaściwym miejscu – o kilka metrów za blisko granicy działki. Powodowało to niezgodność z zatwierdzonym do realizacji projektem i brak możliwości kontynuowania prac.

Jak ustalono, tyczenie przeprowadzono standardowymi metodami za pomocą tachimetru, wykorzystując jako punkty odniesienia kamienie graniczne. Błąd polegał na niewłaściwym odczytaniu wymiaru z mapy zasadniczej przy jednej z granic działki. Po wstępnym wytyczeniu pierwszego punktu wszystkie kolejne wykonano wobec niewłaściwie przyjętego punktu początkowego. Geodeta nie był w stanie wyjaśnić, z czego wynikła tak podstawowa pomyłka.

Na szczęście błąd został wykryty w miarę wcześnie, kiedy nie rozpoczęto jeszcze prac związanych z budową pierwszego piętra budynku. Dlatego roboty naprawcze obejmowały jedynie przebudowę ław fundamentowych oraz częściową rozbiórkę i ponowną budowę ścian parteru, ale już we właściwym miejscu.

Koszt prac związanych z przebudową stanowił dla inwestora nikłą część budżetu przeznaczonego na realizację całej inwestycji. Dla geodety zaś równy był kilkumiesięcznym zarobkom.

DAMNUM EMERGENS, LUCRUM CESSANS

Kolejny przykład dotyczy firmy budowlanej, która zawarła umowę o przeprowadzenie prac ziemnych. Zlecenie polegało na wykonaniu przekopu wzdłuż remontowanej przez głównego wykonawcę drogi. W dniach poprzedzających rozpoczęcie prac zakończono wszelkie niezbędne formalności związane z realizowanym przedsięwzięciem, m.in. ustalono zakres i miejsce pracy, pobrano mapę do celów projektowych z zaznaczonym uzbrojeniem terenu (mapa uprzednio została zatwierdzona przez Zespół Uzgadniania Dokumentacji Projektowej) oraz wydano stosowne wytyczne co do sposobu prowadzenia robót. Ponadto właściciel sieci energetycznej wydelegował swojego pracownika, który miał nadzorować prace wykonywane w pobliżu instalacji. Całość nadzorował także kierownik budowy z ramienia głównego wykonawcy oraz kierownik robót z firmy, która miała prace zrealizować. Przed samym rozpoczęciem zlecenia wykonano przekopy kontrolne, aby móc potwierdzić, czy instalacja podziemna znajduje się w miejscach wskazanych na mapie. Wreszcie zapoznano pracowników z warunkami panującymi na terenie budowy. Po zakończeniu przygotowań ruszyły

roboty. A następnego dnia... doszło do uszkodzenia przyłącza energetycznego prowadzącego do pobliskiego budynku. Dość szybko ustalono przyczynę zdarzenia. Winny okazał się pracownik firmy budowlanej zatrudnionej do wykonania prac ziemnych. Niepomny otrzymanych wytycznych, w momencie gdy natrafił na przeszkodę, uznał, że jest to korzeń rosnącego w pobliżu drzewa i z zawzięciem przystąpił do jego usuwania.

Naprawy przyłącza dokonano w ciągu kilku godzin. Jej koszty stanowiły jedynie część wynagrodzenia, jakie firma budowlana miała otrzymać za realizację powierzonych im prac. Natomiast prawdziwy problem pojawił się kilka dni później. Pobliski budynek, którego przyłącze energetyczne zostało uszkodzone, był zakładem produkcyjnym.

W związku z uszkodzeniem przyłącza doszło do zwarcia, które uszkodziło podzespoły maszyny wykorzystywanej do produkcji. Zatrzymanie maszyny uniemożliwiło dokończenie bieżącego procesu wytwarzania. Zniszczony został obrabiany w chwili zdarzenia materiał, a bieżącą produkcję całkowicie wstrzymano. W efekcie zakład nie dość, że nie zdołał wywiązać się ze swoich umów, to jeszcze został obciążony karami za niezrealizowanie zleceń w terminie.

Specjalistyczna naprawa i ściąganie z zagranicy części potrzebnych do jej wykonania zajęły nerwowe dwa tygodnie. Firma budowlana otrzymała roszczenia przekraczające kilkudziesięciokrotnie wynagrodzenie ujęte w zawartej umowie.

WBREW PRAWU GRAWITACJI

Następny przykład dotyczy firmy sprzątającej. Jej pracownik, jak każdego dnia, przystąpił do swoich obowiązków, gdy ruch w zakładzie pracy, który miał uprzątnąć, już się zakończył. W pewnym momencie natrafił na drobny problem. Szafki, które chciał odkurzyć, były umieszczone zbyt wysoko. Udał się więc do sąsiedniego pomieszczenia po krzesło. Niestety, nie zdążył go nawet donieść. Gdy tylko przekroczył próg pomieszczenia, krzesło nagle wyrwało się z jego rąk... i odleciało. Zdarzenie trwało ułamek sekundy i ostatecznie okazało się nie tak trudne do wyjaśnienia.

Rozwiązaniem zagadki krzesła, które na podobieństwo braci Wrightów postanowiło zostać pionierem awiacji, są szczególne okoliczności zdarzenia. Sprzątanym zakładem pracy był szpital. Natomiast krótka przygoda z lataniem metalowego krzesła zakończyła się jego ugrzęźnięciem w komorze rezonansu magnetycznego.

Ze względu na swoją konstrukcję rezonans nawet w trybie pasywnym wytwarza silne pole magnetyczne. Jego pełne wyłączenie jest możliwe tylko w sytuacjach awaryjnych (np. zagrożenia życia pacjenta) lub w celu przeprowadzenia napraw. W tym przypadku zdarzenie wymagało wizyty specjalistycznego serwisu, który w celu oderwania krzesła od rezonansu musiał zdjąć pole magnetyczne, a następnie dokonać wymiany elementów, które zostały uszkodzone. Samo tylko powtórne włączenie rezonansu wymagało sprawdzenia funkcjonowania magnesu, wykonania procedur rozruchowych oraz uzupełnienia poziomu helu, który uwolnił się bezpowrotnie w momencie wyłączenia zasilania. Szpital musiał także poczekać kilka dni na dostawę części do wymiany.

Wiemy już, jaki przebieg miało zdarzenie, ale dlaczego do niego doszło? Czy pomieszczenie z rezonansem było nieprawidłowo oznakowane? Wprost przeciwnie, oznaczenia były duże i czytelne, a możliwe zagrożenia opisane w pięciu językach. Może pracownik był źle przygotowany? Też nie, przed rozpoczęciem prac przeszedł właściwe szkolenie i był instruowany o potencjalnym ryzyku. Może był niedoświadczony i oszołomiony pierwszymi dniami w nowym miejscu? Niestety, był to pracownik z długoletnim stażem i zaznajomiony ze specyfiką pracy w szpitalu. Do szkody doprowadziła prozaiczna czynność. Pracownik wykonał ją rutynowo, zapominając, gdzie się znajduje.

Bilans strat sięgał setek tysięcy złotych.

GORE

Ostatni przykład dotyczy zdarzenia powstałego podczas planowej przerwy w produkcji, wprowadzonej przez duży zakład wytwórczy. Przestój przedsiębiorstwa miał być wykorzystany

Codziennie przeciętny człowiek wykonuje bezwiednie setki drobnych czynności, nad którymi przeważnie się nie zastanawia.

Fot.: Shutterstock

SPODZIEWANE KORZYŚCI, RZECZYWISTE SZKODY

Zgodnie z art. 361 § 2 Kodeksu cywilnego naprawienie szkody obejmuje straty, które poszkodowany poniósł (damnum emergens), oraz korzyści, które mógłby osiągnąć, gdyby mu szkody nie wyrządzono (lucrum cessans). Stratą po stronie poszkodowanego będzie zarówno zmniejszenie aktywów (np. zniszczenie lub uszkodzenie rzeczy poszkodowanego), jak i zwiększenie pasywów (np. powstanie nowych zobowiązań, co nie miałoby miejsca, gdyby szkody nie wyrządzono). Utracone korzyści natomiast zawsze będą miały charakter hipotetyczny, a ich wykazanie z prawdopodobieństwem graniczącym z pewnością leży po stronie poszkodowanego.

do przeprowadzenia m.in. wszelkiego typu prac remontowo-konserwacyjnych.

Do części prac związanych z rewizją stanu jednej z kluczowych instalacji zatrudniono podwykonawcę. Sama instalacja stanowiła odrębną budowlę porównywalną rozmiarami do średniej wielkości bloku mieszkalnego. Prace powierzone podwykonawcy miały obejmować m.in. wymianę skorodowanych śrub i nakrętek. Ponieważ zatrudnionym ślusarzom nie udało się odkręcić mocno zapieczonych śrub, postanowili do ich wymiany użyć szlifierki kątowej.

Kiedy zauważyli ogień, chwycili za gaśnice. Jednak ich starania okazały się daremne, gdyż pożar rozprzestrzeniał się zbyt szybko. Ugasiła go dopiero zakładowa straż pożarna.

Pożarnik przybyły na pogorzelisko ustalił przyczynę zdarzenia na podstawie śladów zastanych na miejscu oraz relacji świadków. Pożar spowodowały spadające rozżarzone ścinki śrub, od których zapaliły się specjalnie profilowane cienkie arkusze wytworzone z mieszanki opartej na polichlorku winylu. Czysta forma polimeru PVC kwalifikuje się do materiałów samogasnących. Natomiast wszelkie użyte dodatki, mające poprawić właściwości polimeru, przeważnie zwiększają jego palność. Tak też było w tej sytuacji. Użyte arkusze nie były łatwopalne, ale użyta do ich produkcji mieszanka okazała się na tyle podatna na temperaturę, że uległy zapaleniu. Wybuchowi pożaru sprzyjały również kształt paneli oraz dobry dostęp do tlenu.

Spaliła się cała instalacja poddawana konserwacji. Jej odbudowa trwała kilka miesięcy. Straty liczono w milionach złotych.

KALEJDOSKOP ZAGROŻEŃ

Przytoczone sytuacje nie są czymś niecodziennym. Samowolne oddalenie się pracownika z miejsca pracy powoduje przelanie się setek ton paliwa. Brak należytego zabezpieczenia linii produkcyjnej podczas wykonywania prac demontażowych wymusza kilkudniowe wstrzymanie produkcji. Wadliwie wykonana lub nieprawidłowo dokręcona złączka doprowadza do zalania hali wystawienniczej. Uszkodzenie systemu spryskiwaczy ładunkiem przewożonym przez pracownika magazynu doprowadza do zalania sprzętu elektronicznego znacznej wartości...

Codziennie przeciętny człowiek wykonuje bezwiednie setki drobnych czynności, nad którymi przeważnie się nie zastanawia. Są to nieskomplikowane działania, wykonywane automatycznie i choć składają się często na większe ciągi akcji, zwykle nie wymagają znacznej uwagi. Przeważnie nie ma w tym nic złego. Problem pojawia się wtedy, gdy przyzwyczajenia i rutyna przenoszone są w miejsce pracy.

Skala potencjalnych konsekwencji i szkód, jakie niosą ze sobą, wydawałoby się, prozaiczne czynności, jest nie do oszacowania. Opisane przykłady dotyczyły jedynie prostych zleceń, polegających na wykonywaniu stosunkowo nieskomplikowanych prac, ale ich konsekwencje mogłyby zachwiać stabilnością finansową nawet dużej firmy. Mowa tylko o łatwo policzalnych kwestiach pieniężnych. A co z brakiem zaufania ze strony kontrahentów lub utratą renomy albo dobrego imienia spółki?

Pytanie brzmi: czy w świecie, którego złożoność zdaje się rosnąć na naszych oczach, jest miejsce na zastój w postrzeganiu zagrożeń otaczających przedsiębiorcę? Same przykłady zdarzeń można by długo mnożyć, a wniosek od dawna jest ciągle ten sam: jak zaskakująco niewiele trzeba, by doszło do szkody. RF

Rafał Perczak
Główny Specjalista w Biurze Likwidacji Szkód Korporacyjnych, ekspert w zakresie likwidacji szkód OC, absolwent Wydziału Ekonomicznego UG, w Grupie Ergo Hestia od 2008 r.

rafal.perczak@ergohestia.pl

Fot.: STU Ergo Hestia SA

90%

z pierwszych dziesięciu firm branży surowce i paliwa ubezpiecza Ergo Hestia.

wg listy 500 tygodnika Polityka 2012 r.

Ergo Hestia
Jestem pewien

ERGO HESTIA®

Infolinia: **801 107 107**
koszt połączenia wg taryfy operatora

www.ergohestia.pl

BEZPIECZEŃSTWO FLOT
bez uprzedzeń

NICOLAS-JOSEPH CUGNOT JEST UWAŻANY ZA OJCA PIERWSZEGO POJAZDU MECHANICZNEGO NAPĘDZANEGO PARĄ. FRANCUSKI KONSTRUKTOR NIE ZDAWAŁ SOBIE SPRAWY, ŻE PONAD 200 LAT OD PREMIERY JEGO WYNALAZKU OBSŁUGA POJAZDU NIE BĘDZIE WYMAGAŁA... **OBECNOŚCI KIEROWCY**.

Tekst: **Tomasz Tkaczyk**

Rewolucyjne rozwiązanie testowane jest obecnie w USA, ciągle jednak bezpieczna jazda samochodem zależy przede wszystkim od jego stanu technicznego i umiejętności kierowcy. Wokół bezpieczeństwa aut flotowych i ich użytkowników narosło wiele mitów, z którymi musimy mierzyć się na co dzień.

PRZEPIS NA ŻYCIE

Na początek sięgnijmy do art. 3 ustawy Prawo o ruchu drogowym: „Uczestnik ruchu i inna osoba znajdująca się na drodze są obowiązani zachować ostrożność albo gdy ustawa tego wymaga – szczególną ostrożność, unikać wszelkiego działania, które mogłoby spowodować zagrożenie bezpieczeństwa lub porządku ruchu drogowego, ruch ten utrudnić albo w związku z ruchem zakłócić spokój lub porządek publiczny oraz narazić kogokolwiek na szkodę. Przez działanie rozumie się również zaniechanie". Warto zwrócić uwagę na słowo „zaniechanie", które padło w ostatnim zdaniu. Dotyczy ono przede wszystkim kierowców, którzy świadomie lekceważą i łamią przepisy wynikające z Kodeksu drogowego, narażając tym samym siebie i innych na utratę zdrowia lub życia. Użytkownicy aut firmowych biorą udział w co trzecim wypadku drogowym i są sprawcami co drugiej kolizji. Najczęstsze przyczyny to – według policyjnych statystyk – znaczne przekroczenie prędkości, brak reakcji na zmienne warunki pogodowe oraz wymuszanie pierwszeństwa przejazdu na drodze.

Nieco mniejszymi przewinieniami są rozmowy telefoniczne prowadzone bez używania zestawów głośnomówiących, brak włączonych świateł mijania czy niezapięcie pasów bezpieczeństwa. To ostatnie kierowcy często tłumaczą tym, że przez pasy nie mogliby szybko opuścić samochodu w razie pożaru. Mit ten obalają dane: tylko 0,5 proc. wypadków drogowych jest związanych z pożarem pojazdu. Wielu kierowców (zwłaszcza pojazdów ciężarowych) wychodzi z założenia, że po mieście i na krótkich trasach jeździ się wolno, więc w razie wypadku nic im się nie stanie. Po co więc zapinać pasy? Prawa fizyki są nieubłagane. Jeśli samochód jedzie z prędkością 50 km/h, przy zderzeniu ciało kierowcy jest wyrzucane z siedzenia z siłą 1 t. Przy uderzeniu w stałe elementy samochodu skutki mogą być śmiertelne, również dla pasażera siedzącego z przodu.

Inną kwestią jest korzystanie podczas jazdy z telefonów komórkowych. Niektórzy administratorzy flot nie chcą wyposażać aut firmowych w zestawy głośnomówiące, bo uważają, że kierowcy za bardzo skoncentrują się na rozmowach prywatnych zamiast na prowadzeniu samochodu. Fakty są jednak takie, że pracownicy i tak rozmawiają lub piszą SMS-y jedną ręką, prowadząc jednocześnie samochód. A wówczas nie ma mowy o tym, by mogli dostatecznie uważnie kontrolować sytuację na drodze. Jeśli wydarzy się coś nieoczekiwanego, trudno im będzie wykonać sprawny i udany manewr rozpędzonym autem.

Stosowanie i konsekwentne egzekwowanie odpowiednich zapisów w polityce flotowej, zwanej często regulaminem użytkowania pojazdów służbowych, może znacząco podnieść świadomość kierowców w zakresie bezpieczeństwa na drodze. Obowiązkiem zarządzającego parkiem samochodowym jest tworzenie procedur, które uwzględniają najczęstsze zagrożenia dla bezpieczeństwa pojazdów oraz ich użytkowników.

KIEROWCA MILE WIDZIANY...

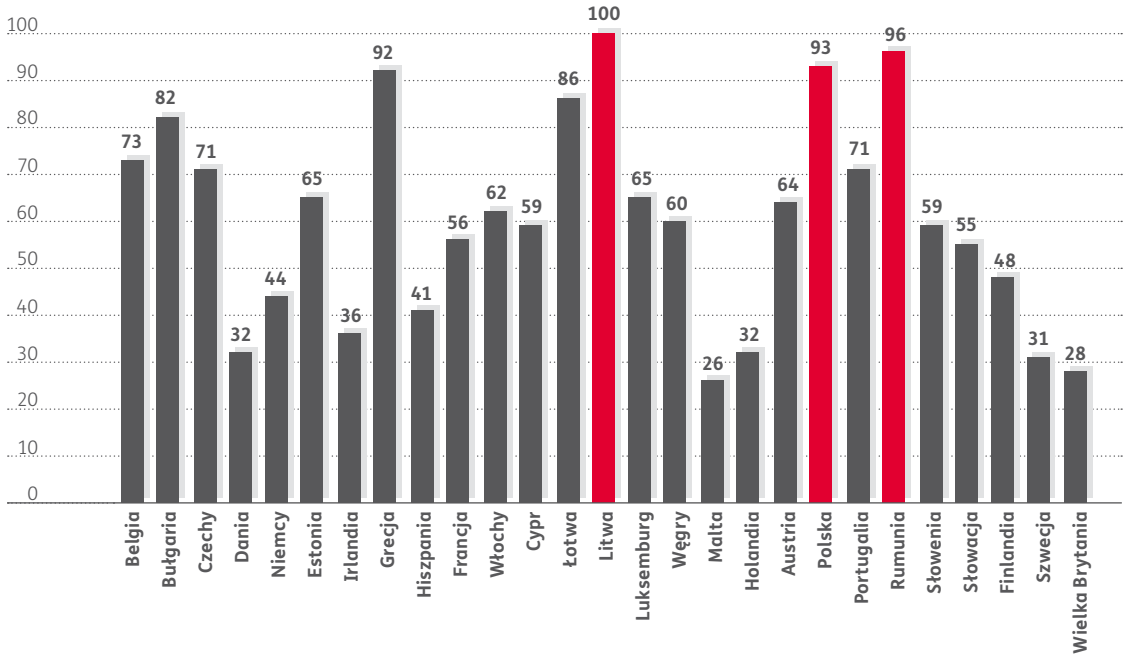
Z kilkuletnim doświadczeniem, powyżej 25. roku życia, regularnie uczestniczący w ruchu drogowym i... najlepiej mężczyzna. Z takimi oczekiwaniami najczęściej można się zetknąć w ogłoszeniach prasowych czy internetowych. Czy kobiety faktycznie częściej powodują kolizje lub wypadki drogowe? Baba za kierownicą – oto jeszcze jeden stereotyp. Łatwo go obalić za pomocą statystyk Polskiej Izby Motoryzacji. Panie o wiele rzadziej niż panowie łamią przepisy. Nawet 59 proc. kobiet nigdy(lub bardzo rzadko) nie przekracza dozwolonej prędkości (do ograniczeń prędkości stosuje się natomiast tylko 45 proc. panów), 35 proc. kobiet nigdy nie przekracza linii ciągłej, a 45 proc. nie wymusza pierwszeństwa. Wśród panów te wskaźniki wynoszą odpowiednio 27 proc. i 40 proc. Nie powinny więc dziwić dane Komendy Głównej Policji, która ogłosiła, że w 2012 r. kobiety były sprawcami 20 proc. wszystkich wypadków na polskich drogach. To pozostawia 75,7 proc. wypadków spowodowanych przez płeć brzydką (w 4,3 proc. przypadków nie określono, kto był sprawcą).

Mimo że perspektywy znalezienia pracy w branży transportowej, logistycznej, komunikacyjnej są niezłe, rekrutacja kierowców – zwłaszcza w transporcie międzynarodowym – ciągle przysparza menedżerom

>>

Fot.: Shutterstock

LICZBA OFIAR ŚMIERTELNYCH NA MILION MIESZKAŃCÓW W 2012 R.



Źródło: Komisja Europejska

flotowym niemało kłopotu. Firmy potrafią kusić kierowców lepszymi zarobkami, nowoczesnymi pojazdami czy atrakcyjnymi warunkami pracy, co powoduje dużą rotację osób w tej branży. Flotowcy mierzą się z problemem znalezienia odpowiedzialnego, bezszkodowego i rzetelnego pracownika. Najczęściej zatrudnia się osoby polecone przez bardziej doświadczonych, zaufanych pracowników. Okres próbny trwa przeważnie bardzo krótko i obejmuje przejazdy w charakterze zmienników kierowców, zapoznawanie się z trasami, obsługą auta i specyfiką pracy.

Należy jednak pamiętać, że posiadanie uprawnień do prowadzenia danej jednostki mechanicznej nie daje gwarancji, że kandydat ma odpowiednie predyspozycje czy pożądane umiejętności. O tych niestety pracodawcy dowiadują się dopiero po rozpoczęciu współpracy. Bagatelizowanie weryfikacji umiejętności kierowców w zakresie bezpiecznego uczestnictwa w ruchu drogowym może dla floty oznaczać bardzo wysokie koszty ekonomiczne, kadrowe, moralne lub wizerunkowe. Dlatego coraz częściej sięga się po narzędzia sprawdzające przyszłych kierowców w zakresie znajomości budowy auta oraz jego użytkowania.

Wzorowym działaniem jest organizowanie testów drogowych dla przyszłych pracowników. Również tych, dla których auto będzie codziennym narzędziem pracy (przejazdy z punktu A do punktu B). Wspomniane testy można organizować przy współpracy z instruktorami z lokalnych ośrodków jazdy, wykwalifikowanymi egzaminatorami lub osobami zarządzającymi pojazdami, posiadającymi duże doświadczenie i wiedzę.

W przypadku pojazdów wielkogabarytowych szczególną uwagę należy zwrócić na umiejętność prawidłowego ruszania i włączania się do ruchu, a także skręcania, cofania i parkowania, sygnalizowania manewrów i zachowania odległości od pojazdów poprzedzających. Cofanie i parkowanie aut wydają się kluczowe. Bardzo dużo szkód powstaje właśnie podczas wykonywania tych manewrów w miastach o dużym natężeniu ruchu, z małą liczbą miejsc parkingowych, wąskimi ulicami i drogami jednokierunkowymi. Kierowcy muszą więc dysponować wysokimi umiejętnościami, chłodną głową oraz wyczuciem odległości, aby nie narażać pracodawców na koszty związane z naprawą samochodów i przestojami w pracy.

SAMOCHÓD SŁUŻBOWY, NAJLEPSZY WÓZ TERENOWY...

Faktem jest, że samochód służbowy to narzędzie pracy, ale zarazem duża wartość dodana dla pracownika. Polski rynek na przestrzeni ostatnich kilku lat odnotowuje znaczny wzrost liczby pojazdów zapewnianych pracownikowi przez pracodawcę. Można założyć, że taki trend będzie się utrzymywał. Czy pracownik, który otrzymuje do dyspozycji samochód, będzie o niego należycie dbał, nie narażając swojego pracodawcy na dodatkowe koszty związane z nadmierną eksploatacją i uszkodzeniami? Wielu kierowców wychodzi z założenia, że samochód służbowy to pojazd, który „sam się tankuje, sam naprawia,", a koszty z tym związane są przecież wliczone w ryzyko jego użytkowania. Dlatego nie trzeba się martwić, gdzie się go parkuje i jak się z niego korzysta...

Wyobraźmy sobie, że posiadamy flotę 200 pojazdów. Każdy z nich jest eksploatowany nadmiernie i nieostrożnie. W ciągu roku rosną koszty eksploatacji do kwoty rzędu 2-3 tys. zł, ponieważ należy wymieniać szybciej zużywające się opony, układy hamulcowe, elementy zawieszenia,

Fot.: STU Ergo Hestia SA

nie wspominając o nadmiernym zużyciu paliwa lub drobnych uszkodzeniach blacharsko-lakierniczych. Jak temu przeciwdziałać? Jednym z programów prewencyjnych jest system motywacyjny. Może on obejmować np. możliwość pierwokupu pojazdu służbowego przez jego użytkownika po wycofaniu auta z floty firmowej. Jest to jedna z najprostszych, ale też najskuteczniejszych metod. Co może lepiej przekonać kierowcę, by jeździł samochodem ostrożnie, niż perspektywa, że kiedyś auto będzie należeć do niego? Można również prowadzić wewnątrzfirmowy ranking kierowców, promujący właściwe postawy. Kto jeździ najlepiej i najostrożniej, zostanie nagrodzony wymianą pojazdu na nowy lub wyższej klasy czy z lepszym wyposażeniem. Zamiennie można też zastosować nagrody finansowe wypłacane miesięcznie, kwartalnie lub raz w roku. Nie należy zapominać o drugiej stronie systemu motywacyjnego, który obok nagród za rozważną i bezpieczną eksploatację powinien zawierać taryfikator kar dla kierowców nieroztropnie korzystających z przydzielonego im mienia firmowego. Tu także mamy do wyboru kilka narzędzi. Można zastosować takie kary jak udział własny w finansowaniu napraw, utrata premii czy potencjalnych nagród, otrzymanie auta niższej klasy, degradacja stanowiska pracy albo utrata możliwości korzystania z pojazdu do celów prywatnych. To oczywiście tylko wybrane przykłady.

Można sobie zadać pytanie o to, co jest bardziej skuteczne: nagrody czy kary. Otóż i w tym przypadku warto zastosować złoty środek, pozwalający na elastyczność i dopasowanie środków do charakteru kierowców – i tych mniej chętnych do współpracy, i tych, którzy lubią współzawodnictwo czy doceniają wagę korzyści, jakie mogą odnieść dzięki trosce o służbowe auto.

BYĆ JAK ROBERT KUBICA

Około 80 proc. polskich kierowców uważa, że jeździ dobrze lub bardzo dobrze. Wśród nich nie brakuje kierowców pojazdów flotowych. Wielu z nich oczami wyobraźni widzi się w mistrzostwach świata Formuły 1, najbardziej prestiżowych zawodach na świecie, w których całkiem niedawno startował Robert Kubica. Swoich sił próbują na polskich torach, przesuwając wskazówki prędkościomierzy w nieosiągalną dla spowalniaczy jazdy stronę. Łatwo więc odpowiedzieć na pytanie, co jest najczęstszą przyczyną wypadków w Polsce. Pod względem liczby ofiar śmiertelnych na milion mieszkańców – według danych Komisji Europejskiej za 2012 r. – nasz kraj plasuje się w ścisłej czołówce tego niechlubnego rankingu (dane na wykresie). Wyprzedzają nas jedynie Litwini i Rumuni. Statystyki dowodzą, że nasi kierowcy jeżdżą szybko i brawurowo, zbyt pewni własnych umiejętności, co z kolei prowadzi do ciężkich wypadków, w których giną inni uczestnicy ruchu drogowego albo postronne osoby.

Problem za szybkiej jazdy nie omija oczywiście firm. W przypadku pojazdów ciężarowych działaniem prewencyjnym może być montaż ograniczników prędkości. W samochodach osobowych batem na rajdowe zapędy kierowców jest monitorowanie przejazdów za pomocą systemu GPS oraz wprowadzanie działań motywujących i przemawiających do rozsądku. Coraz częściej zdarza się, że administratorzy flot korzystają z wiedzy i doświadczenia szkół bezpiecznej jazdy, co przekłada się na większą świadomość, wyższe umiejętności i bezpieczniejsze zachowanie pracowników.

Eksperci prowadzący zajęcia doskonalące technikę jazdy wskazują na trzy podstawowe błędy popełniane przez użytkowników pojazdów mechanicznych. Są nimi: nieprawidłowa ocena sytuacji, błędna decyzja i styl prowadzenia pojazdu. Zaawansowane ćwiczenia mogą skorygować błędne nawyki nabyte jeszcze podczas kursów prawa jazdy. Podstawowe zajęcia obejmują przejazdy po śliskim, mokrym torze (na podobieństwo trudnych, zaskakujących warunków występujących na drodze), manewrowania na zakrętach z luźno zamocowanymi tylnymi kołami, próby wyprowadzenia auta z niekontrolowanego poślizgu czy operowanie hamulcem.

Niektórzy flotowcy podchodzą dość sceptycznie do szkoleń teoretyczno-praktycznych z udziałem własnych kierowców. Część z nich uważa, że takie zajęcia jeszcze bardziej umocnią pracowników w przekonaniu o wielkim talencie do prowadzenia pojazdów. W odpowiedzi warto przytoczyć wypowiedź jednego z użytkowników auta firmowego na temat uczestnictwa w szkoleniu bezpiecznej jazdy.

„Uważałem się za doskonałego kierowcę, zanim po raz pierwszy nie skorzystałem z możliwości sprawdzenia swoich umiejętności w warunkach kontrolowanego poślizgu pojazdu oraz wykonywaniu innych, niespodziewanych manewrów. Okazało się, że moje wyobrażenie i posiadana teoria nijak się nie mają do faktycznie posiadanej wiedzy i umiejętności. Opiszę jedno z ćwiczeń weryfikujących moje mylne założenie o własnej doskonałości. Pusta płyta lotniska, na jej środku przygotowana tzw. płyta poślizgowa mająca imitować zachowanie pojazdu na mokrej nawierzchni. Na jej środku ustawiono przeszkodę, którą należy ominąć, zachowując właściwy tor jazdy. Rozpędzam pojazd do prędkości 80 km/h. Przecież bardzo często jeździmy właśnie z taką prędkością poza miastem. Byłem w pełni przygotowany i odpowiednio skoncentrowany. Wiedziałem, co powinienem zrobić, aby ominąć przeszkodę. Mimo to została ona zmieciona z powierzchni lotniska, a po próbie jej ominięcia pojazd wykonał kilka obrotów wokół własnej osi i znalazł się około 10 m z lewej strony teoretycznie wykreślonego pasa ruchu. Na szczęście każda kolejna próba była już znacznie lepsza, aż w końcu po którymś ćwiczeniu udało się bezbłędnie ominąć przeszkodę i pozostać z pojazdem w pasie ruchu. Wyobraźmy sobie zatem, że do podobnej sytuacji dochodzi nieoczekiwanie na drodze, a my nie mamy ani wystarczających umiejętności, ani doświadczenia…” RF

Tomasz Tkaczyk
Hestia Loss Control, specjalista ds. oceny ryzyka, zajmuje się zagadnieniami bezpieczeństwa flot pojazdów. Z wykształcenia inżynier, absolwent Wydziału Mechanicznego Politechniki Gdańskiej. W Grupie Ergo Hestia od 2006 r.

tomasz.tkaczyk@ergohestia.pl

KONFERENCJA

IDENTYFIKACJA ZAGROŻEŃ JAKO PODSTAWA OCENY RYZYKA
6. OGÓLNOPOLSKA KONFERENCJA MIESIĘCZNIKA ATEST

NAMIERZ ZAGROŻENIE, zmniejsz ryzyko

Jak uniknąć błędów w ocenie ryzyka? Identyfikacja zagrożeń będzie tematem przewodnim konferencji organizowanej przez redakcję miesięcznika „Atest”.

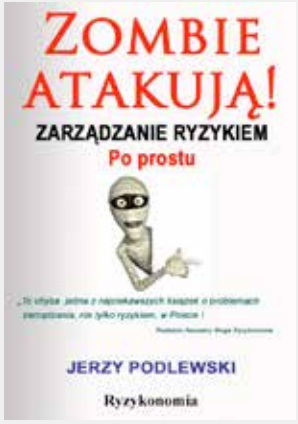
Nie można oszacować ryzyka bez kompleksowej, pogłębionej analizy potencjalnych zagrożeń – fizycznych, chemicznych, biologicznych i psychospołecznych. Istnieje wiele metod ich identyfikacji i pomiaru – o wszystkich opowiedzą eksperci zaproszeni do udziału w konferencji „Identyfikacja zagrożeń jako podstawa oceny ryzyka”. To szósta z kolei ogólnopolska konferencja organizowana przez magazyn „Atest” – organizatorzy zachęceni pozytywnym odzewem po poprzedniej edycji postawili na rozwój formuły wydarzenia: zaplanowano więcej ekspertów, rozszerzony zakres tematyczny udzielanych przez nich porad. Na konferencji zostaną omówione takie zagadnienia jak: metody identyfikacji ryzyka, zagrożenia na stanowiskach pracy w branży budowlanej, zagrożenia związane z użytkowaniem wyposażenia, zagrożenia elektromagnetyczne, metody doboru środków ochrony indywidualnej, błędy medyczne, zagrożenia w świetle dyrektywy SAVESO II i SAVESO III, identyfikacja zagrożeń i ocena ryzyka w przemyśle chemicznym. Konferencja odbędzie się w dniach 13-15 listopada w Krakowie.

6. Ogólnopolska Konferencja Miesięcznika „Atest” – „Identyfikacja jako podstawa zagrożeń ryzyka”, 13-15.11.2013

KSIĄŻKA

Jerzy Podlewski,

Zombie atakują! Zarządzanie ryzykiem po prostu



Jaki apetyt na ryzyko miał Czerwony Kapturek? Dlaczego firmy bankrutują, a ich menedżerowie nie piszą o tym książek? Czy równouprawnienie zwiększa ryzyko w biznesie? Jak profesjonalnie przygotować się na nadejście żywych trupów?

To tylko niektóre z wielu zaskakujących pytań, na które odpowiedzi można znaleźć w książce „Zombie atakują! Zarządzanie ryzykiem po prostu”. Autor w niezwykle prosty, zrozumiały i często zabawny sposób wyjaśnia różnorodne aspekty związane z zarządzaniem ryzykiem i zachowaniem ciągłości działania. To pozycja polecana wszystkim tym, którzy szukają sposobów na radzenie sobie z ryzykiem wszechobecnym w biznesie i życiu prywatnym. To książka o zarządzaniu ryzykiem... po prostu.

Fot.: materiały promocyjne

Bezpieczna jazda:
Podróż zapięta na ostatni guzik!

ERGO HESTIA rekomenduje

Po co używać pasów bezpieczeństwa?

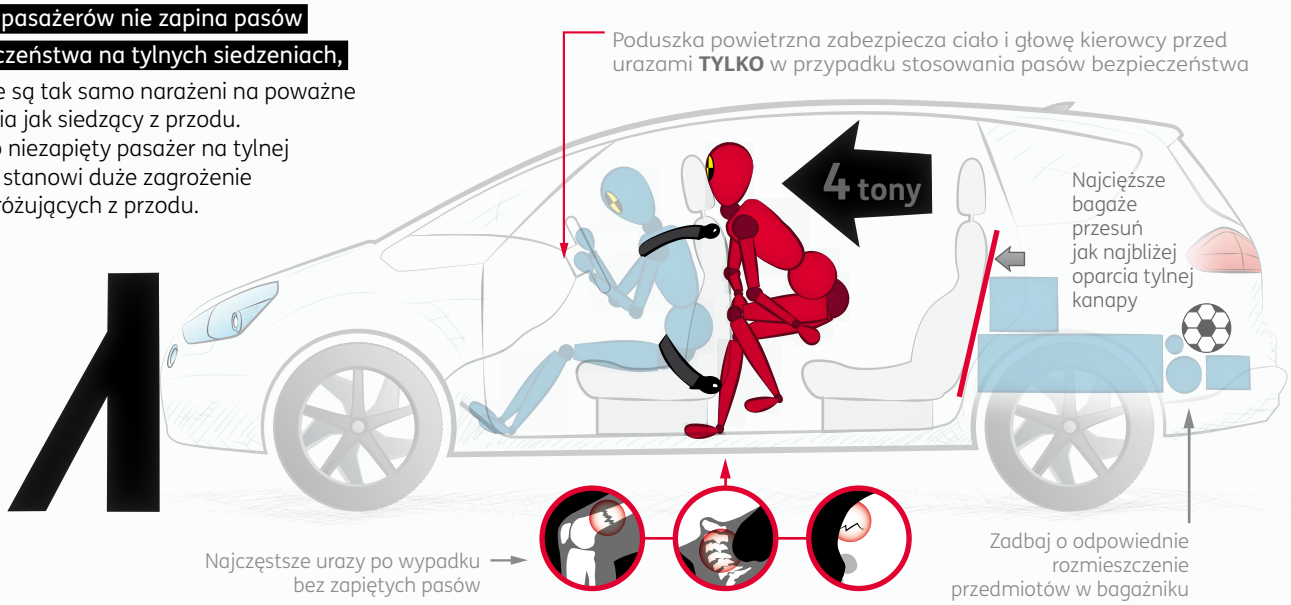
Przy czołowym zderzeniu niezapięty pasażer siedzący z tyłu, może przełamać oparcie przedniego fotela i zmiażdżyć osobę na nim siedzącą. **Jadąc 50 km/h w chwili zderzenia z nieruchomą przeszkodą „masa zderzeniowa" pasażera wzrasta 50 razy!**

60%

aż tylu pasażerów nie zapina pasów bezpieczeństwa na tylnych siedzeniach, mimo że są tak samo narażeni na poważne obrażenia jak siedzący z przodu. Ponadto niezapięty pasażer na tylnej kanapie stanowi duże zagrożenie dla podróżujących z przodu.

Jak się zabezpieczyć?

- **Zanim ruszysz upewnij się, że wszyscy pasażerowie zapięli pasy**
- **Pamiętaj aby górna krawędź zagłówka sięgała przynajmniej czubka głowy**
- **Zadbaj o odpowiednie rozmieszczenie przedmiotów w bagażniku**



Zwiększ bezpieczeństwo swoje oraz pasażerów!

Pamiętaj o prawidłowym zapięciu pasów bezpieczeństwa. Powinny:

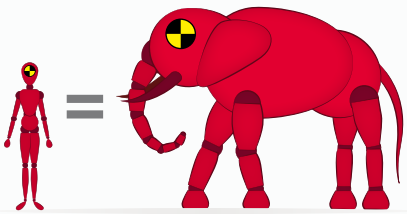
- płasko przylegać do ciała
- opinać biodra jak najniżej w stosunku do brzucha
- przebiegać nad środkiem barku, bez tendencji do zsuwania się z ramienia

Nie kładź ciężkich przedmiotów (np. torby) na siedzeniu pasażera – w razie wypadku czujniki identyfikują ciężar na fotelu i mogą uruchomić poduszkę powietrzną pasażera

Nie kładź parasola lub innych przedmiotów na tylnej półce – w chwili zderzenia polecą do przodu stanowiąc śmiertelne zagrożenie dla pasażerów.

Wyobraź sobie – jesteś kierowcą, a za Tobą siedzi słoń...

Przy **50 km/h** w chwili zderzenia „masa zderzeniowa" pasażera wzrasta **50 razy!**



Zapnij pasy, unikniesz mandatu!

Od 1991 r. obowiązek zapinania pasów obowiązuje również na tylnych siedzeniach oraz wszystkich rodzajach dróg

100 zł tyle zapłaci kierowca za **niezapięcie pasów bezpieczeństwa**. Tyle samo zapłacimy przewożąc pasażerów bez zapiętych pasów.

150 zł taki mandat otrzymają **przewożący dzieci poza fotelikiem** ochronnym lub w foteliku, ale tyłem do kierunku jazdy na przednim siedzeniu pojazdu wyposażonego w aktywną poduszkę powietrzną dla pasażera.

HLC

Hestia Loss Control

Audyt ryzyka

- ogień i inne zdarzenia losowe
- uszkodzenia maszyn i urządzeń
- ryzyko utraty zysku
- OC za produkt
- OC za szkody środowiskowe
- bezpieczeństwo flot pojazdów

Wycena wartości majątku do celów ubezpieczeniowych

- budynki i budowle
- maszyny i urządzenia

Doradztwo

- koncepcje zabezpieczeń budynków i urządzeń
- plany zachowania ciągłości działania
- plany wycofywania produktu z rynku

Szkolenia i warsztaty

- zarządzanie ryzykiem
- ocena wybranych kategorii ryzyk
- przedsięwzięcia prewencyjne

ERGO HESTIA®

Ergo Hestia
Jestem pewien

Infolinia: **801 107 107**
koszt połączenia wg taryfy operatora

www.ergohestia.pl