BEZPIECZEŃSTWO • 2019 nr 4
TEORIA I PRAKTYKA

e-ISSN 2451-0718
ISSN 1899-6264

DOI: 10.34697/2451-0718-btip-2019-4-007

Mirosław Laszczak

dr inż., Wyższa Szkoła Ekonomiczno-Humanistyczna w Bielsku-Białej
ORCID: 0000-0001-6060-4285

Zarządzanie bezpieczeństwem w erze cyfrowej

Wprowadzenie

Postępująca cyfryzacja zmieniła gospodarkę. Przestrzeń i czas utraciły swój bezwzględny paradygmat, a dostęp do informacji i przetwarzanie danych stało się łatwe jak nigdy wcześniej. Nie bez powodu mówi się o rewolucji cyfrowej przenicowującej kulturę, ekonomię, a przede wszystkim świadomość. Świat nie jest już taki przed pięćdziesięciu laty – warunki prowadzenia biznesu trudno porównywać nawet do tych z końca XX w. Cyfryzacja przeorała każdą dziedzinę życia, dokonując nieodwracalnej konwergencji wirtualnego i rzeczywistego świata. Pojawia się internet rzeczy (*Internet of Things*, IoT) – będący siecią przedmiotów, procesów i ludzi ciągle podłączonych do internetu. Dochodzi do hiperkomunikacji (*hyperconnectivity*). Urządzenia bez przerwy przetwarzają ogromne ilości informacji (*big date analylics*, BDA), a część usług dokonuje się w obliczeniowej chmurze (*cloud computing*). Normą staje się automatyzacja i robotyzacja. Przyzwyczailiśmy się do wielokanałowości i wszechkanałowości dystrybucji produktów (*omni channel*). Przez 24 godziny na dobę konsumenci korzystają z cyfrowego dostępu do dóbr i usług (*digital customer access*).

Obserwowane zmiany mają charakter rewolucyjny, formy biznesu znane z poprzedniego stulecia stają się nie tylko niewydolne, ale wręcz nie przystają do nowych czasów. Wiele osób, także tych, którzy zarządzają przedsiębiorstwami, nie do końca zdaje sobie sprawę z charakteru dokonujących się zmian. Coraz więcej informacji przetwarzanych jest poza umysłem decydenta, intuicja przestała mieć znaczenie, a pomiędzy zarządzającymi i konsumentami pojawili się informatycy, korzystający z systemów tak złożonych, że dla większości użytkowników niezrozumiałych.

Przez ostatnich pięćdziesiąt lat moc obliczeniowa procesorów podwaja się z każdym mijającym rokiem. Koszty przetwarzania informacji maleją w tym samym tempie, a co dwa lata pojawia się więcej informacji niż w całej wcześniejszej historii. Bez ustanku generujemy nowe informacje, łączymy się z bankami, wysyłamy wiadomości tekstowe, publikujemy prace naukowe, a przede wszystkim w zapisie binarnym składujemy dane finansowe. W każdym dowolnym momencie ktoś dokonuje operacji bankowych, a liczbę sprzedanych smartfonów mierzy się w miliardach. Nie należy się łudzić – biznesowe połączenia są smakowitym kąskiem nie tylko dla domorosłych przestępców rekrutujących się spośród znudzonych studentów informatyki. Kradzieżą informacji zajmują wyspecjalizowane działy poważnych i praworządnych zdawałoby się instytucji. Firma General Electric wielokrotnie skarżyła się na podsłuchiwanie przez zagranicznych konkurentów. Po koniec lat 80. XX w. przegrała wiele przetargów w Europie, czasem różnicą zaledwie kilku tysięcy dolarów. Wynajęci przez firmę eksperci dość szybko znaleźli przyczynę: konkurenci uważnie śledzili satelitarną łączność General Motors i podsłuchiwali rozmowy. Firma zakupiła wówczas tak zwane telefony bezpieczne, szyfrujące połączenia. Wydatek rzędu stu tysięcy dolarów opłacił się: GE znowu zaczęła wygrywać przetargi na Starym Kontynencie[1].

Ten i podobne przypadki utorowały drogę nowemu myśleniu o bezpieczeństwie w czasach powszechnej informatyzacji, komputeryzacji i digitalizacji zarchiwizowanych danych. Stało się jasne, że należy wyjść poza znane dotychczas metody bronienia dostępu do zgromadzonej w organizacji wiedzy, a sposób ochrony winien przyjąć formę systemowego zarządzania bezpieczeństwem.

Celem niniejszego artykułu jest przedstawienie niebezpieczeństw związanych z powszechną cyfryzacją gospodarki oraz wskazanie podstawowych elementów odpowiedzialnych za bezpieczeństwo organizacji na poziomie cyfrowym. Przyjęto hipotezę badawczą, zgodnie z którą zarządzanie bezpieczeństwem w erze cyfrowej odbiega od klasycznych konotacji związanych z tym pojęciem, gdyż koncentruje się na zagrożeniach wynikłych z informatyzacji procesów zarządzania i komunikowania się ze światem zewnętrznym. Zarządzanie bezpieczeństwem w erze cyfrowej wymaga podejścia systemowego i oprócz sprecyzowania zbioru najważniejszych zasad, konieczna jest koncentracja wysiłków na kluczowych i dających się wyodrębnić obszarach aktywności organizacji.

Formy zagrożeń

Przechytrzyć system, wedrzeć się poza zaporę bezpieczeństwa i nie ruszając się z fotela, uzyskać dostęp do cudzych pieniędzy lub zastrzeżonych informacji. W 2008 r. świat obiegła interesująca wiadomość. W ręce amerykańskiej policji wpadł haker, który wniknął do systemu informatycznego sieci marketów i jednocześnie przeniknął do firmy produkującej karty kredytowe. Nie ruszając się z domu skradł – bagatela − 130 mln USD. Oczywiście nie działał sam, do dyspozycji miał gang zorganizowany z nastoletnich hakerów, którzy nie znalazłszy dla siebie zatrudnienia

[1] P. Schweizer, *Szpiedzy wśród przyjaciół. Jak sojusznicy wykradają Amerykanom tajemnice technologiczne*, tłum. J. Lobman, Z. Słomkowski, Warszawa 1997, s. 287.

pośród „białych kapeluszy”[2], zdecydowali się wykorzystywać swe umiejętności w mniej szlachetny sposób. Ze swobodą poruszali się w galimatiasie informatycznych komend, wynajdywali luki w systemach komputerowych, włamywali się na konta bankowe i przejmowali tajne informacje. Wśród zatrzymanych znajdował się młody człowiek, który jako nastolatek zhakował komputery NASA, za co otrzymał wyrok sześciu miesięcy poprawczaka. Ktoś taki i jemu podobni nigdy nie przestaną buszować w sieci; w ten sposób zaspakajają atawistyczne pragnienie polowania – o tyle wygodnie, że nie trzeba ruszać się z domu, można siedzieć w ulubionym fotelu, jeść pizzę i popijać colę. Młodzi informatycy, dla których sieć jest labiryntem z oznaczonymi ścieżkami, mają szansę na udowodnienie intelektualnej przewagi nad twórcami zabezpieczeń. Zabawa miesza się z przygodą, przyzwyczajenie zahacza o uzależnienie, a łatwość dużego zarobku kusi. Z czasem hakerzy okazali się także prawdziwymi specjalistami od ludzkiej psychiki. Zwerbowani przez nich przeciętni konsumenci zostali się „słupami” przyjmującymi przelewy i depozyty bankowe oraz wysyłającymi je do odległych geograficznie banków. Ten rodzaj oszustwa rozpowszechnił się w 2009 r.: banki i ich klienci stracili wówczas znacznie ponad 120 mln USD[3].

Współcześnie nie ma już kraju, firmy ani organizacji, które nie byłyby zagrożone hakerskim atakiem. W sukurs nieczystym intencjom idą technologie pomagające zachować anonimowość w sieci. Jedną z nich jest sieć TOR (The Onion Router) działająca w najbardziej zakamuflowanych i najciemniejszych miejsca w sieci. Pozwala ona na anonimowe korzystanie z dostępnych zasobów w sieci powierzchniowej, a także ułatwia dostęp do zaszyfrowanych treści[4]. Czy może zatem dziwić dynamika wzrostu przestępczości internetowej?

Komenda Główna Policji informuje, że w 2018 r, w porównaniu z rokiem 2017 nastąpił stuprocentowy wzrost liczby przestępstw odnoszących się do e-bankowości i phishingu.

Tabela 1. Wzrost liczby przestępstw dotyczących bankowości elektronicznej na tle ogólnej liczby przestępstw bankowych

Rok	**2014**	**2017**	**2018**
Przestępstwa o charakterze bankowym	2,5 tys.	6 tys.	7,4 tys.
Przestępstwa z zakresu phishingu i e-bankowości	585	1,8 tys.	3,6 tys.
Skimming*	brak danych	433	743

* przestępstwo polegające na nielegalnym skopiowaniu karty płatniczej (np. poprzez umieszczenie dodatkowego czytnika i nadajnika w konstrukcji bankomatu).

Źródło: opracowanie własne na podstawie: W. Boczoń, *100 proc. wzrost liczby przestępstw dotyczących e-bankowości. Statystyki policji*, PRNews.pl, https://prnews.pl/100-proc-wzrost-przestepstw-dotyczacych-e-bankowosci-statystyki-policji-441137 [dostęp: 12.06.2019].

[2] „Białe kapelusze” to hakerzy, którzy sprawdzają oprogramowanie pod kątem luk w zabezpieczeniach, a znalezione niedoróbki zgłaszają producentowi, aby pomóc uszczelnić program i zabezpieczyć go przed ingerencją tych „złych” – czyli „czarnych kapeluszy”.

[3] K. Poulsen, *Haker. Prawdziwa historia szefa cybermafii*, tłum. T. Macios, Kraków 2011, s. 266.

[4] A. Nastuła, *Fałszerstwo dokumentów ze szczególnym uwzględnieniem przestępczości internetowej jako wyzwanie dla organów państwa*, „Polonia Journal” 2018, nr 8, s. 80–83.

Banki oraz ich klienci atakowani są na różne sposoby. Oprócz tradycyjnego phishingu przestępcy wykorzystują jego mutacje, sięgają więc po vishing i smishing. Dochodzi do wyłudzeń z wykorzystaniem Blika i metody SIM-swap[5], tworzone są fałszywe aplikacje bankowe, które wzbudzają zaufanie, gdyż udostępniane są w markecie Google Play.

Nieskończona jest pomysłowość oszustów, którzy z sieci informatycznych uczynili wygodne narzędzie, o tyleż bardziej perfidne, że bazujące na naiwności i braku wiedzy niektórych użytkowników, wierzących w tajemną moc systemów informatycznych i bezgranicznie ufających witrynom internetowym.

Zagrożeń jest tak wiele, że jakakolwiek ich lista nigdy nie będzie kompletna. Ogólnie wyróżnia się[6]:

- kradzież lub niszczenie danych,
- podszywanie się pod inną osobę, kradzież wizerunku,
- propagowanie fałszywych informacji, tworzenie wirtualnych organizacji z myślą o dokonywaniu wyłudzeń,
- sabotaż i szantaż komputerowy,
- hacking,
- szpiegostwo komputerowe,
- piractwo komputerowe i kradzież myśli technicznej,
- manipulacje finansowe, w tym przede wszystkim fałszowanie operacji rozrachunkowych, dokonywanie zmian w stanach kont, malwersacje z użyciem kart bankomatowych,
- oszustwa teleinformatyczne i telekomunikacyjne.

Szczególnym rodzajem zagrożeń jest APT (*advanced persistent threats*), będący zorganizowanym, niemal masowym atakiem na systemy informatyczne. Obiektem ataków są zazwyczaj organizacje o kluczowym znaczeniu dla gospodarki. Ofiarami padają instytucje finansowe, organizacje społeczne, rządowe, systemy energetyczne i wojskowe. Forma ataku jest wielostopniowa i bardzo dobrze zakamuflowana. Rzadko kiedy chodzi wyłącznie o pieniądze, częściej – o sparaliżowanie ważnej gałęzi gospodarki, zaszantażowanie instytucji, a jeszcze częściej o szpiegostwo[7]. Ten rodzaj ataków stanowi jedno z największych niebezpieczeństw, nie dziwi zatem, że jest wykorzystywany w konfliktach międzypaństwowych. Za pomocą APT udaje się wywołać chaos i zakłócić obieg pieniądza w gospodarce, można uzyskać przewagę ekonomiczną i militarną, doprowadzić do sparaliżowania systemów

[5] Phising – metoda polegająca na wysyłaniu fałszywych e-maili (pochodzących jakoby z banku), informujących o konieczności pilnego przekazania poufnych danych lub przelania kwoty na określony rachunek; vishing – telefoniczne wyłudzanie danych wrażliwych (numerów kont, loginów, haseł, kodów dostępu) pod pozorem ich weryfikacji, audytu zewnętrznego lub modernizacji systemu komputerowego; smishing – wysyłanie fałszywych SMS-ów nakłaniających ofiarę do połączenia z podanym numerem lub wejścia na określoną stronę internetową, zawierającą np. wirusy i trojany; SIM-swap – oszustwo polegające na wyrabianiu duplikatu karty SIM telefonu służącego do autoryzacji transakcji w systemach bankowości internetowej i wyprowadzaniu w ten sposób środków z konta.

[6] M. Nowak, *Cybernetyczne przestępstwa – definicje i przepisy prawne*, „Biuletyn EBIB" 2010, nr 4 (113), http://www.ebib.pl/2010/113/a.php?nowak [dostęp: 12.06.2019].

[7] I. Ghafir, V. Prenosil, *Advanced Persistent Threat Attack Detection: An Overview*, [w:] *Proceedings of International Conference on Advances in Computing, Electronics and Electrical Technology*, Kuala Lumpur 2014, s. 154, www.seekdl.org/nm.php?id=3901 [dostęp: 12.06.2019].

obronnych. W dodatku jest to atak trudny do odparcia, a generowane straty są poważne: zniszczeniu mogą ulec zgromadzone dane, serwery stają się niewydolne, następuje utrata łączności ze światem zewnętrznym. Dodatkowo trzeba uwzględnić całkiem realną kradzież informacji – w takiej sytuacji możliwe materialne i wizerunkowe szkody są trudne do oszacowania.

Wyróżnia się dwa zasadnicze rodzaje cyberataków:

- DDoS – czyli atak z zamiarem zablokowania serwisów i dokonania kradzieży danych;
- kradzież informacji wrażliwych z myślą o późniejszym publikowaniu ich w sieci, głównie w serwisach i portalach społecznościowych.

Szczególnym miejscem, w którym kumulują się ryzyka związane z cyberprzestępczością, jest chmura. *Cloud computing*, czyli przetwarzanie informacji na zewnątrz organizacji, może budzić zrozumiały niepokój, tym bardziej że:

- wciąż ograniczone są możliwości egzekwowania wymogów bezpieczeństwa na najwyższym poziomie u właścicieli chmury;
- organizacje, z którymi dana organizacja wymienia się informacjami, stanowią zagrożenie dla ochrony informacji zdeponowanych w chmurze;
- brakuje dobrze ustrukturalizowanej architektury i strategii rozwoju środowiska chmury, która gwarantowałaby stuprocentowe bezpieczeństwo zdeponowanych danych;
- występują luki w interfejsie obsługi. Za bezpieczeństwo API (*application programming interface*) odpowiadają dostawcy usług chmurowych, natomiast wykorzystanie kluczy, które powiązane są z interfejsami programistycznymi, znajduje się w gestii użytkowników usług chmurowych[8];
- wymóg korzystania wyłącznie ze sprawdzonych usługodawców nie zawsze może być spełniony.

Nie tylko wielość oraz różnorodność przestępstw w cyberprzestrzeni sprawia, że statystyki policyjne nie są dokładne. Wpływają też na to inne przyczyny:

- nie wszystkie przestępstwa zostają zgłoszone;
- dane ujawniają jedynie naruszenia prawa otagowane przez policjantów jako cyberprzestępstwo, w rzeczywistości nie wszystkie przypadki otrzymują tego typu opis;
- od wejścia w życie obowiązującej ustawy o świadczeniu usług drogą elektroniczną[9] z 2002 r. w technologii cyfrowej minęła cała epoka. Część popełnianych obecnie przestępstw nie była znana w czasie przygotowywania ustawy.

Wbrew obiegowym opiniom kradzieże bankowe, choć niewątpliwie bolesne, nie są największą zmorą osób odpowiedzialnych za bezpieczeństwo w sieci. Wykradanie informacji biznesowych i danych wrażliwych, transfer technologii – staje się problemem więcej niż palącym.

Słabość informatycznych zabezpieczeń ma dwa źródła. Pierwszym są luki w systemach komputerowych, które choćby i dokładnie sprawdzone, zawsze będą

---

[8] P. Waszczuk, *11 zagrożeń dla bezpieczeństwa rozwiązań chmurowych według Cloud Security Alliance*, https://itwiz.pl/11-zagrozen-dla-bezpieczenstwa-rozwiazan-chmurowych-wedlug-cloud-security-alliance [dostęp: 12.06.2019].

[9] Ustawa z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną, Dz.U. z 2002 r., nr 144, poz. 1204.

zawierać błędy pozostawione przez programistów. Drugim – jeszcze poważniejszym – jest sam człowiek ze swym roztargnieniem, lenistwem, ze swymi przyzwyczajeniami i skłonnością do robienia wszystkiego na skróty. Dotyczy to nawet pracowników, którzy na co dzień zajmują się bezpieczeństwem przesyłania danych w systemach informatycznych. Wystarczy na dowolnej stronie otworzyć *Sztukę infiltracji* Kevina D. Mitnicka i Williama L. Simona[10], by przekonać się o ludzkich słabościach, nazbyt łatwo wystawiających na szwank dane wrażliwe o trudnej do przecenienia wartości – i w swej nieroztropności narażających mienie tysięcy osób.

Ludzie zajmujący się bezpieczeństwem w branżach IT nie są w stanie pracować ciągle na najwyższych obrotach, wyczulona pierwotnie wrażliwość z czasem słabnie, ostrożność ulega stępieniu. Praca nie jest już wyzwaniem, lecz rutyną. Pracownicy przychodzą do swoich biur, siadają w wygodnych obrotowych fotelach, sprawdzają pocztę, przeglądają ulubione strony www i ani myślą o drobiazgowym sprawdzaniu logów, aby dowiedzieć się, kto przez noc zmienił hasło. Niewiele pomagają szkolenia. Wciąż są tacy, którzy dają się nabrać na starą sztuczkę z podrzuconym pendrive'em. Przypadkowo znaleziony (lecz celowo podrzucony) np. na parkingu nośnik danych uruchamiany jest na firmowych komputerach. Umieszczone na pendrivie szpiegowskie oprogramowanie natychmiast przenika do systemu całej instytucji. Niefrasobliwość bierze górę nad zasadami bezpieczeństwa, ciekawość dominuje nad zdrowym rozsądkiem. A wszystko to dzieje się przy pełnej świadomości niebezpieczeństwa związanego z uruchamianiem plików nieznanego pochodzenia, w instytucjach wysyłających pracowników na drogie szkolenia z bezpieczeństwa.

Nie trzeba jednak przypadkowo znalezionego pendrive'a. Pracownicy nazbyt łatwo przynoszą do pracy własne, domowe nośniki danych. Zabierają pracę do domu, chcą się pochwalić zdjęciami z wakacji, może zamierzają wydrukować w firmie prywatny dokument – możliwości jest bez liku, a z każdą związane jest niebezpieczeństwa zainfekowania systemu.

W grę wchodzi jeszcze jedno, wcale nie tak marginalne niebezpieczeństwo: chęć łatwego zarobku. „Jeśli tylko zaoferuje się odpowiednią cenę, wszyscy pracownicy, począwszy od dyrektora, a na gońcach i sprzątaczkach kończąc, okazują się potencjalnymi szpiegami"[11] – przekonuje jeden z konsultantów do spraw bezpieczeństwa. Nie bez wpływu na postawę pracowników jest panująca w firmie kultura organizacyjna oraz pewien rodzaj przyzwolenia na kradzież informacji. W zalewie danych, gdy codziennie mamy do czynienia z niekończącym się strumieniem informacji, gdy wydaje się, że jest ich tak wiele, że stają się bezwartościowe, trzeba doprawdy bardzo silnego charakteru lub bardzo restrykcyjnych kar, aby powstrzymać pracowników przed bagatelizowaniem poufnych wiadomości. Ważne są oczywiście przyzwyczajenia zawodowe i rozumienie samego pojęcia lojalności. U Amerykanów jest z tym różnie. Łatwo ich przekonać do wyniesienia poufnych danych. Osobiste kłopoty finansowe i nagłe potrzeby gotówkowe czynią z nich

[10] K.D. Mitnick, W.L. Simon, *Sztuka infiltracji*, tłum. C. Frąc, Warszawa 2006. Mitnick to były haker, skazany na wiele lat więzienia. W swojej książce opisuje techniki włamań i podkreśla, że najsłabszym ogniwem najdroższych i najbardziej wyrafinowanych systemów zabezpieczeń jest zawsze człowiek.

[11] P. Schweizer, *op. cit.*, s. 47.

stosunkowo łatwe źródło informacji. Nieuprawnione przekazywanie danych sojusznikom traktują co najwyżej jako formę wstydliwej transakcji. Dopiero przekazywanie informacji agentom rosyjskim lub chińskim jest uznawane za znacznie poważniejszy uszczerbek na honorze i złamanie obywatelskich norm[12].

Jak to wygląda w Polsce? Obserwacje nie są optymistyczne. Lojalność polskich pracowników jest niepewna i efemeryczna – bo i zatrudnienie bywa krótkotrwałe, uzależnione od wynagrodzenia, z opcją opuszczenia obecnego pracodawcy, gdy tylko pojawi się lepsza propozycja.

O ile *baby boomers* i pracownicy z pokolenia X szukają stałego zatrudnienia i wielce pociąga ich wizja pracy w jednym miejscu aż do emerytury, o tyle 63 % młodszych pracowników, w wieku pomiędzy 18 a 35 lat, nie wyobraża sobie, że zestarzeją się, pracując w jednej firmie[13]. Takie podejście osłabia lojalność, co dokumentują statystyki przestępczości. Według danych z 2018 r. połowa polskich przedsiębiorców zetknęła się w ciągu poprzednich dwóch lat z przypadkami nadużyć, z tego ponad połowę (55 %) popełnili zatrudnieni w firmie pracownicy[14].

Najbardziej wrażliwe na ataki cyberprzestępców są innowacyjne firmy oraz instytucje finansowe, zwłaszcza banki. Przeprowadzone przez Institute of International Finance i McKinsey & Company badania ujawniły, że 70 % banków uważa ryzyko związane z cyberatakami za główne zagrożenie, na które należy uwrażliwiać menedżerów średniego szczebla, 10 % ankietowanych stawia ten rodzaj ryzyka na czele listy wszelkich zagrożeń[15]. Nic dziwnego, że co trzeci bank w Europie czwartą część swojego budżetu na obniżanie ryzyka bankowego przeznacza na zarządzanie ryzykiem cyfrowym.

Bezpieczeństwu nie sprzyjają towarzyszące cyfryzacji współczesne trendy, zgodnie z którymi dąży się do jak najszerszego otwarcia na potrzeby klienta i dba się o zwiększenie dostępności usług.

Pierwszym takim trendem jest personalizacja dostępu. E-commerce i dostęp poprzez media społecznościowe jest jak wołanie: „Mamy dla was zawsze otwarte drzwi, zajrzyjcie, sprawdźcie, rozejrzyjcie się". Niechcący zaprasza się w ten sposób także osoby niepożądane, wraz z ich niszczycielskimi narzędziami i dążeniami. Drugi rynkowy trend odnosi się do nacisku konkurencji. W przypadku bankowości są to instytucje pożyczkowe, parabankowe. Chcąc sprostać wymaganiom klientów, banki uruchamiają nowe rozwiązania, nie zawsze właściwie zabezpieczone, a bywa, że przygotowane zbyt pospiesznie. Kolejnym trendem jest pogoń za obniżką kosztów. Informatyka znacznie w tym pomaga. Część czynności wykonują sami klienci – logują się na kontach, organizują przelewy – zastępując rzeszę pracowników.

---

[12] *Ibidem*, s. 48.

[13] Randstad, *Monitor Rynku Pracy*, 35 edycja, 2019, [za:] *Rośnie zadowolenie pracowników, maleje ich lojalność*, PRNews.pl, https://prnews.pl/rosnie-zadowolenie-pracownikow-maleje-ich-lojalnosc-444497 [dostęp: 12.06.2019].

[14] M. Klimczak, *Kto i jak okrada polskie firmy? 8. edycja badania przestępczości gospodarczej w Polsce*, PwC Polska, https://www.pwc.pl/pl/publikacje/2018/badanie-przestepczosci-gospodarczej-2018-raport-pwc.html [dostęp: 12.06.2019].

[15] *The future of risk management in the digital era*, McKinsey & Company, https://www.mckinsey.com/business-functions/risk/our-insights/the-future-of-risk-management-in-the-digital-era [dostęp: 14.06.2019].

Czwarty trend jest ściśle związany z poprzednim i wynika wprost z nowego modelu biznesu. Informatyczne kanały przepływu informacji, funduszy i wiedzy oraz możliwość dotarcia do nich z dowolnego miejsca na świecie czyni je wrażliwymi na cyberataki. Trend piąty to deregulacje. Ułatwianie dostępu klientom, chęć zdobycia ich zaufania, upraszczanie procedur – za tym wszystkim idą deregulacje, ustępstwa, które mogą wystawiać na szwank bezpieczeństwo instytucji. I doprawdy trudno ustalić granicę pomiędzy konieczną sztywnością reguł, które utrudniają współpracę z klientem, a otwarciem się na klienta i sprowokowaniem niepotrzebnego ryzyka. Przecież rezygnacja z możliwości, jakie daje gospodarka cyfrowa, i pominięcie wymogu marketingowego podejścia do klienta, byłaby krokiem w tył. Klienci przyzwyczaili się do przyjaznych systemów, w których wpłat, wypłat i innych operacji dokonuje się łatwo i szybko, bez utrudnień i dodatkowych weryfikacji – które byłyby ceną za zwiększenie szczelności systemu. Jest też trend szósty: część funkcji związanych z bezpieczeństwem zostało przerzuconych na wyrafinowane systemy informatyczne. Nie człowiek, lecz skomplikowane i dla większości ludzi niezrozumiałe oprogramowanie stoi na straży bezpieczeństwa. Tyle tylko, że ufność w te systemy może być przesadzona. Wciąż pojawiają się doskonalsze narzędzia hakerskie, a i pomysłowość cybernetycznych przestępców zdaje się nie mieć granic. Dlatego od samego początku, gdy tylko pojawili się hakerzy, byli oni przekupywani przez firmy i zatrudniani z myślą o poprawie bezpieczeństwa.

Działania zaradcze

Nie ma oprogramowania doskonale chroniącego zdigitalizowane informacje. Nic nie da stuprocentowej pewności, że zarządzający systemami informatycznymi będą lojalni i czujni. Mylne jest przeświadczenie, że jakieś doraźne działania (jak choćby kupno lepszego pakietu informatycznego) zabezpieczają przed cyberprzestępstwami. Gdy zagrożenie jest realne i totalne, trzeba tworzyć kompleksowe zabezpieczenia. W takim przypadku mówi się o zarządzaniu ryzykiem cyfrowym (*digital risk management*). Jest to o tyle trudne, że zagrożenia mogą pojawić się w każdej chwili i w dowolnym miejscu. Ich źródło może tkwić w czynniku ludzkim, materialnym i wirtualnym.

Funkcję zapór bezpieczeństwa, niczym średniowieczne fosy, pełnią obecnie firewalle. Osoba, która nimi administruje, sprawdza konfigurację zapory, przygląda się logowaniom, identyfikuje ewentualne nielegalne zmiany. Ktoś, kto zinfiltruje zaporę sieciową, dokona także innych zmian w systemie i zapewni sobie dostęp do zastrzeżonych informacji. Największym grzechem administratora jest ufność w program komputerowy i w szczelność zapory. Z upływem czasu zawsze ujawnią się jej słabości. Naprawa w jednym miejscu prowadzi do powstania dziur gdzieś indziej. Niektóre porty pozostają niepotrzebnie otwarte, a serwery sieci web bywają źle skonfigurowane. Dlatego żaden firewall nigdy nie jest całkowicie szczelny. Gościnność, chęć stworzenia środowiska pracy, które jest przyjazne dla pracowników i partnerów biznesowych, rozmywa granice ochrony. Internetowi przestępcy szukają szczelin i luk, rozglądają się za słabościami, korzystając – przynajmniej na początku – z legalnych środków i przyjazności samego programu.

Wiele przedsiębiorstw stosuje programy odnotowujące próby włamań i zapobiegające infiltracji. Wszyscy oczekują, że te programy poradzą sobie same. Tymczasem są procedury, których firewall nie chroni. Wynika to z wygody używania sprzętu komputerowego, z posiadanych uprawnień, czasem z konieczności komunikowania się ze światem zewnętrznym i pobierania z zewnątrz pakietów danych. Dlatego tak ważne jest konstruowanie reguł, dzięki którym można filtrować pakiety przychodzące i wychodzące.

Firewalle skonfigurowane są już w taki sposób, aby identyfikować skanowanie portów z myślą o włamaniu. System samoczynnie odłącza takie połączenia oraz informuje o tego typu aktywności – ale tylko jeśli zastosowana przez hakera technika nie jest zbyt wyrafinowana. Stąd cały zestaw zaleceń dla personelu zajmującego się bezpieczeństwem. Chodzi o sprawdzanie listy procesów z intencją wykrycia tych, które nie są znane. Przeczesuje się programy w poszukiwaniu nieautoryzowanych dodatków. W plikach szuka się zmodyfikowanych binariów, skryptów i aplikacji. Usuwa się konta uśpione i nieznane. Reaguje się wzmożoną uwagą na zdalny dostęp z nieznanego miejsca.

Przezorni administratorzy nie ufają domyślnym konfiguracjom. Gdy instalują oprogramowanie pochodzące od zewnętrznej „niezależnej" firmy, z góry zakładają, że w programie znajdują się rozwiązania o charakterze szpiegowskim. Dotyczy to przede wszystkim przedsiębiorstw działających w branży finansowej, w branżach zaawansowanych technologii tudzież w przemyśle wojskowym, farmaceutycznym i biotechnologii. Dokonać infiltracji atrakcyjnej rynkowo firmy i poznać jej sekrety – to nie lada gratka i całkiem zyskowny interes.

Administratorzy co jakiś czas organizują spotkania z pracownikami: instruują ich, uczulają na zagrożenia, podają zbiory zasad. Część z tych zasad jest najczęściej ignorowana i obchodzona. Pracownicy wciąż nazywają pliki zgodnie z ich zawartością, wskazując drogę osobom zainteresowanym infiltracją. Każdy haker zajrzy przede wszystkim do plików opisanych jako „wyniki badań", spenetruje „kopie bezpieczeństwa", pomijając „harmonogram urlopów". Szyfrowanie plików poufnych jest wymogiem, od którego nie może być odstępstw. Istnieją do tego specjalne programy, oczywiście można je obejść i odszyfrować tajne informacje, wiąże się to jednak z koniecznością nieco dłuższego przebywania w sieci, a wszelka manipulacja przy tego typu plikach prędzej lub później obudzi jednak czujność administratora.

Lata wojny pomiędzy hakerami a zatrudnionymi w firmie informatykami oraz „białymi kapeluszami" nie pozostały bez wpływu na podniesienie standardów bezpieczeństwa. Teraz już wiadomo, że po zainstalowaniu oprogramowania koniecznie trzeba usunąć skrypty instalacyjne. Zdarzało się bowiem, że hakerzy zdobywali listy adresowe, wykorzystując słabości w domyślnym skrypcie instalacyjnym aplikacji.

Ryzyko cyfrowe a zarządzanie bezpieczeństwem

Cyberprzestrzeń jest tyleż intratnym, co wygodnym obszarem do działań przestępczych. Jest też obszarem wrażliwym, gdyż nawet niewielka ingerencja w zgromadzone dane uruchamia lawinę strat. Powiązane z sobą różnorodne formy ryzyka, niemal jak ułożone kostki domina, uruchamiają lawinę zdarzeń o trudnych do

wyobrażenia konsekwencjach. Rodzajów ryzyka jest tu bardzo wiele, wystarczy wymienić najważniejsze:

- ryzyko utraty dobrego imienia,
- ryzyko utraty wiarygodności,
- ryzyko kradzieży danych o charakterze badawczo-rozwojowym,
- ryzyko utraty danych klientów i narażenie się na procesy sądowe,
- ryzyko modyfikacji danych,
- ryzyko wycieku danych,
- ryzyko uszkodzenia systemów informatycznych,
- przerwa w działalności,
- ryzyko utraty pozycji rynkowej.

Wyłudzanie informacji, podszywanie się pod cudzą tożsamość, stawanie się „słupem" w nielegalnym procederze prania pieniędzy to kolejne, wcale nierzadkie zdarzenia. Dlatego także informatyka dopracowała się swojej definicji ryzyka – pod postacią normy IEC 61508, zgodnie z którą jest ono miarą zagrożenia tajności, integralności i dostępności informacji. Ryzyko należy traktować jako iloczyn prawdopodobieństwa wystąpienia sytuacji stwarzającej zagrożenie i skutków wyrażonych w wielkości poniesionych strat.

Stąd już tylko krok do zdefiniowania systemu zarządzania bezpieczeństwem danych, który znany jest jako norma ISO/IEC 27001[16]. Norma ta stała się punktem wyjścia dla tworzenia systemów zarządzania bezpieczeństwem informacji (*Information Security Management System*, ISMS). Istota zarządzania sprowadza się do utrzymywania ryzyka na poziomie akceptowalnym przez organizację, czyli zapewniającym efektywne osiąganie celów biznesowych przy jednoczesnym nienarażaniu na szwank rzeczowych i niematerialnych składników organizacji. Zarządzanie próbuje skłonność do ryzyka pogodzić z otwarciem się na potrzeby klienta, a sprawną interakcję pomiędzy rynkiem i organizacją – z długofalowym bezpieczeństwem.

Zarządzanie ryzykiem przyjmuje dwie formy[17]:

1) prewencji – rozumianej jako przygotowanie organizacji na cyberataki, monitorowanie sieci w organizacji, sprawdzanie podatności na zagrożenia, identyfikowanie możliwych zagrożeń,
2) minimalizacji strat wynikłych z cyberataków.

Prewencja jest tu najważniejsza. O tyle o nią trudno, że część zagrożeń nie jest nawet znana, część metod – nie dość rozpoznana, a kreatywność cyberprzestępców nie ma sobie równych. Najłatwiej określić podstawowy zestaw działań zaradczych. W grę wchodzi bowiem reglamentacja dostępu do sprzętu, oprogramowania, sieci zewnętrznych i wewnętrznych, a przede wszystkim – wglądu do zgromadzonych informacji. Ważne jest także ustalenie wymogów jakościowych odnośnie do sprzętu

[16] ISO/IEC 27001:2013(en): *Information technology – Security techniques – Information security management systems – Requirements*, https://www.iso.org/obp/ui/#iso:std:iso-iec:27001:ed-2:v1:en [dostęp: 12.06.2019].

[17] E.I. Szczepankiewicz, P. Szczepankiewicz, *Analiza ryzyka w środowisku informatycznym do celów zarządzania ryzykiem operacyjnym*, cz. 3: *Strategie postępowania z ryzykiem operacyjnym*, „Monitor Rachunkowości i Finansów" 2006, nr 8, https://czasopisma.beck.pl/monitor-rachunkowosci-i-finansow/artykul/analiza-ryzyka-w-srodowisku-informatycznym-do-celow-zarzadzania-ryzykiem-operacyjnymbr-czesc-3-strategie-postepowania-z-ryzykiem-operacyjnym [dostęp: 12.06.2019].

i oprogramowania. Usługi IT zlecane czy wykonywane siłami samej organizacji to także jeden z obszarów, gdzie często dochodzi do powstania ryzykownych sytuacji. Nie można zapominać o aktualnych i odpowiednio sprawnych systemach wykrywania i usuwania złośliwego oprogramowania. Poprzestanie na uaktualnionej wersji programu antywirusowego może nie wystarczyć, warto go dostosować do specyfiki prowadzonej działalności. Organizacje ubezpieczają się od szkód, ale chyba najistotniejsze są szkolenia dla personelu i ugruntowane mechanizmy kontroli wewnętrznej. Nie daje to oczywiście stuprocentowej pewności, lecz znacznie utrudnia pracę cyberprzestępcom.

Kiedy już dojdzie do ataku hakerskiego, nie pozostaje nic innego jak uruchomić działania minimalizujące szkody. Przebiegają one wielotorowo i obejmują:

- aktywność marketingową, podejmowaną głównie przez dział PR z zadaniem zniwelowania ewentualnych strat wizerunkowych,
- identyfikację i szacowanie poniesionych szkód,
- ustalenie przyczyny, źródła wycieku danych i winowajców,
- wyodrębnienie puli środków na ewentualne odszkodowania,
- jak najszybsze uruchomienie planów awaryjnych i wdrożenie działań naprawczych,
- skorzystanie z urządzeń zapasowych (backupów).

Próbę skonstruowania modelu zarządzania bezpieczeństwem podjęto w firmie doradczej McKinsey & Company. Nie zbudowano co prawda spójnej koncepcji, wskazano jednak na zbiór elementów uważanych za podstawowe w dążeniu do zmniejszenia ryzyka[18].

Wszystko zaczyna się na poziomie zarządzania danymi. Posiadane przez przedsiębiorstwo informacje podlegają ścisłej klasyfikacji, dokonuje się taksonomicznych podziałów, uwzględnia wartość i wagę posiadanych danych, a następnie przypisuje do nich poziom ryzyka. Jest on zmienny, zależny od ilości danych, od źródeł ich pochodzenia i od sposobu wykorzystania. W nadmiarze informacji kryje się poważne niebezpieczeństwo. Gdy jest ich bardzo dużo, przestaje się dostrzegać ich wyjątkowość i rangę, a stąd tylko krok do ignorowania zasad bezpieczeństwa.

Drugim składnikiem zarządzania bezpieczeństwem cyfrowym jest automatyzacja i komputeryzacja procesów. Przywykliśmy już, że łącząc się z firmą, w słuchawce słyszymy przede wszystkim głos z automatu. Od tej tendencji nie ma odwrotu, czynnik kosztowy wygrywa. Klienci i kontrahenci samodzielnie wprowadzają dane do systemu, dzięki temu mają wrażenie, że wszystko dzieje się szybciej, że panują nad toczącymi się procesami. Dane te przechodzą następnie do środowiska pracy, są dostępne w dowolnym miejscu na niemal dowolnym stanowisku. Jest to znaczące udogodnienie, lecz równocześnie wzrasta możliwość penetracji systemu informatycznego. Jeśli firma wpuszcza do sieci każdego, kto tylko zechce, musi liczyć się z tym, że oprócz klientów znajdzie się tam haker, próbujący przetestować własne pomysły na cudzych zabezpieczeniach.

Na trzeci element zarządzania bezpieczeństwem składają się zaawansowane techniki analizowania procesów. Wyrafinowane algorytmy, samouczące się oprogramowanie − wysublimowane narzędzia informatyczne są tu stosowane z myślą

[18] *The future of risk management…*

o wynajdywaniu złożonych wzorców zachowań charakterystycznych dla niedozwolonych transakcji i komputerowych oszustw. Takie narzędzia są ogromnie pomocne. Menedżerowie zatrudnieni w banku są przekonani, że skraca to procedury kredytowe i wpływa na zmniejszenie zatrudnienia. W bankowych oddziałach nie trzeba już zatrudniać tak wielu pracowników. Dzięki szerokopasmowym łączom i podłączeniom do różnorodnych baz danych klienci w krótkiej chwili zostają „prześwietleni" – i okazują się bardziej lub mniej wiarygodni. Również możliwość pomyłki jest tu zapewne mniejsza, aniżeli wówczas, gdy ryzyko kredytu miałby ustalać pracownik banku. Ostateczna decyzja bazować będzie na danych pozyskanych z każdego rodzaju aktywności potencjalnego kredytobiorcy, nie ujdą uwadze nawet dokonywane przez niego zakupy w hipermarkecie. Informatyczne algorytmy podpowiedzą, jaką decyzję podjąć, zdejmując część troski o bezpieczeństwo z zatrudnionych w banku pracowników.

Takie działania nie byłyby możliwe bez rozwoju cybernetycznej infrastruktury. Spójna, elastyczna, bezpieczna, wygodna staje się koniecznością − i to zarówno z marketingowego, jak i technicznego punktu widzenia. Komfortowe, intuicyjnie działające interfejsy, łatwiejszy dostęp do kontrahentów, innowacyjne rozwiązania przechowywania i udostępniania danych, do tego ciągła łączność i podtrzymywanie wszystkich elementów systemu staje się podstawą każdej sprawnie działającej organizacji. Zarządzanie bezpieczeństwem sprowadza się do ustalenia równowagi pomiędzy wygodą użytkowania systemów a możliwością pojawienia się chętnych do ingerencji w infrastrukturę.

W systemie zarządzania bezpieczeństwem cyfrowym nie można pominąć jeszcze jednego elementu. Chodzi o podejście do ryzyka samych pracowników[19]. Posługiwanie się na co dzień terminologią ryzyka biznesowego i świadomość zagrożeń przenosi się na bezpieczeństwo funkcjonowania firmy we współczesnym, zdigitalizowanym świecie. Lecz wcale nie jest tak, że korzystanie z wyrafinowanych programów komputerowych usuwa pracowników w cień, zdejmuje z nich część odpowiedzialności za bezpieczeństwo cyfrowe. Wręcz odwrotnie, nabierają oni kluczowego znaczenia. Liczy się ich wykształcenie i doświadczenie zawodowe – im bardziej różnorodne, tym lepiej. Istotne, by pracownicy uwzględniali zagrożenia w swej bieżącej pracy i przebywali w kulturze organizacyjnej ceniącej eksperymentowanie. Przydaje się ich obycie z systemami informatycznymi i z pracą polegającą na obróbce informacji. W ten sposób odpowiednia polityka rekrutacyjna oraz szkolenia podnoszą bezpieczeństwo cyfrowe, a przy okazji obniżają koszty prowadzenia działalności – osoby zatrudnione na co dzień w firmie są o wiele tańsze niż zewnętrzni specjaliści i eksperci, którzy często nie znają specyfiki danego miejsca i charakteru przetwarzanych w nim informacji.

Mądra postawa pracowników staje się tym ważniejsza, gdy w grę wchodzi zagrożenie wynikające z ataków socjotechnicznych – przed którymi nie zabezpiecza żaden program antywirusowy i które są najtrudniejsze do wykrycia.

[19] Mówią też o tym przywoływane badania, zob. *ibidem*.

Podsumowanie

Nawet pobieżne przejrzenie statystyk zaskakuje dynamiką przyrostu liczby ataków hakerskich, ich różnorodnością i pomysłami przenikania przez szczelne zapory firewalli. Wzrasta liczba destrukcyjnych oddziaływań na systemy informatyczne pojedynczych firm i instytucji rządowych. Cyberprzestępczość wyszła z kart powieści fantastycznych i zadomowiła się w gospodarce. W sukurs przychodzą coraz doskonalsze systemy wykrywania niechcianych ataków, przedsiębiorstwa uczą się minimalizowania ryzyka. Dziś wiadomo, że dbałość o bezpieczeństwo jest trwałym składnikiem procesu zarządzania i wymaga traktowania systemowego. Świadome tego zarządy tworzą wyspecjalizowane komórki organizacyjne, a uczelnie – wychodząc naprzeciw oczekiwaniom rynku – uruchamiają nowe kierunki i specjalności koncentrujące się na zarządzaniu bezpieczeństwem. Bo choć nie da się wyeliminować zagrożeń, to podejście systemowe i doskonalenie zarządzania w kluczowych obszarach odpowiedzialnych za ryzyko umożliwiają prowadzenie stabilnego biznesu we współczesnej, coraz bardziej zdigitalizowanej erze.

Bibliografia

Boczoń W., *100 proc. wzrost liczby przestępstw dotyczących e-bankowości. Statystyki policji*, PRNews.pl, https://prnews.pl/100-proc-wzrost-przestepstw-dotyczacych-e-bankowosci-statystyki-policji-441137 [dostęp: 12.06.2019].

Ghafir I., Prenosil V., *Advanced Persistent Threat Attack Detection: An Overview*, [w:] *Proceedings of International Conference on Advances in Computing, Electronics and Electrical Technology*, Kuala Lumpur 2014, www.seekdl.org/nm.php?id=3901 [dostęp: 12.06.2019].

Klimczak M., *Kto i jak okrada polskie firmy? 8. edycja badania przestępczości gospodarczej w Polsce*, PwC Polska, https://www.pwc.pl/pl/publikacje/2018/badanie-przestepczosci-gospodarczej-2018-raport-pwc.html [dostęp: 12.06.2019].

Mitnick K.D., Simon W.L., *Sztuka infiltracji*, tłum. C. Frąc, Warszawa 2006.

Nastuła A., *Fałszerstwo dokumentów ze szczególnym uwzględnieniem przestępczości internetowej jako wyzwanie dla organów państwa*, „Polonia Journal" 2018, nr 8.

Nowak M., *Cybernetyczne przestępstwa – definicje i przepisy prawne*, „Biuletyn EBIB" 2010, nr 4 (113), http://www.ebib.pl/2010/113/a.php?nowak [dostęp: 12.06.2019].

Poulsen K., *Haker. Prawdziwa historia szefa cybermafii*, tłum. T. Macios, Kraków 2011.

Rośnie zadowolenie pracowników, maleje ich lojalność, PRNews.pl, https://prnews.pl/rosnie-zadowolenie-pracownikow-maleje-ich-lojalnosc-444497 [dostęp: 12.06.2019].

Schweizer P., *Szpiedzy wśród przyjaciół. Jak sojusznicy wykradają Amerykanom tajemnice technologiczne*, tłum. J. Lobman, Z. Słomkowski, Warszawa 1997.

Szczepankiewicz E.I., Szczepankiewicz P., *Analiza ryzyka w środowisku informatycznym do celów zarządzania ryzykiem operacyjnym*, cz. 3: *Strategie postępowania z ryzykiem operacyjnym*, „Monitor Rachunkowości i Finansów" 2006, nr 8, https://czasopisma.beck.pl/monitor-rachunkowosci-i-finansow/artykul/analiza-ryzyka-w-srodowisku-informatycznym-do-celow-zarzadzania-ryzykiem-operacyjnymbr-czesc-3-strategie-postepowania-z-ryzykiem-operacyjnym [dostęp: 12.06.2019].

The future of risk management in the digital era, McKinsey & Company, https://www.mckinsey.com/business-functions/risk/our-insights/the-future-of-risk-management-in-the-digital-era [dostęp: 14.06.2019].

Waszczuk P., *11 zagrożeń dla bezpieczeństwa rozwiązań chmurowych według Cloud Security Alliance*, https://itwiz.pl/11-zagrozen-dla-bezpieczenstwa-rozwiazan-chmurowych-wedlug-cloud-security-alliance/ [dostęp: 12.06.2019].

Zarządzanie bezpieczeństwem w erze cyfrowej
Streszczenie

Era cyfrowa, przez przyspieszenie wymiany informacji i zmianę formy obiegu dokumentów, stworzyła nowe wejścia do przedsiębiorstw i urzędów. Już nie oszklone frontowe drzwi, lecz internetowe łącza prowadzą w głąb organizacji. Pracowników ochrony zastąpiły komputerowe systemy zabezpieczenia informacji, programy antywirusowe i firewalle. Światłowodami można dotrzeć znacznie dalej, przeniknąć w struktury organizacji nieporównanie głębiej i wyrządzić szkody wielokrotnie większe od tych, które mogli poczynić „klasyczni" złoczyńcy.

Zagrożeń jest tak wiele, że nie sposób ich wszystkich wymienić, a codziennie powstają nowe formy ataku i nieznane wcześniej sposoby wyłudzeń informacji i pieniędzy. Początkowo tworzono zbiory zasad, z którymi zaznajamiano pracowników. Dotyczyły one ochrony kopii i plików poufnych, sposobów tworzenia haseł dostępu, postępowania z informacjami. W stosunkowo krótkim czasie okazało się jednak, że ochrona przed cyberprzestępczością domaga się systemowego potraktowania. Pojawiło się pojęcie zarządzania bezpieczeństwem w erze cyfrowej – zagadnienie to jest usystematyzowane i skoncentrowane na jasno wyodrębnionych obszarach. Obejmuje: zarządzanie danymi, zarządzanie procesem przepływu informacji, zautomatyzowane procesy decyzyjne, zarządzanie infrastrukturą, inteligentne interfejsy, zarządzanie zewnętrznym „ekosystemem" informatycznym i zarządzanie umiejętnościami pracowników oraz kulturą organizacyjną. Koncentracja na tych obszarach na pewno nie wyeliminuje zagrożeń, lecz znacząco poprawi bezpieczeństwo, od którego często zależy dalsze trwanie organizacji.

Słowa kluczowe: era cyfrowa, bezpieczeństwo, cyberprzestępczość, zarządzanie bezpieczeństwem, ochrona danych

Security Management in the Digital Era
Abstract

The digital era, accelerating the exchange of information and changing the form of document circulation, have created new entrances to any organisations. No longer the glazed front door, but internet links lead someone deep into the organization. Guards and security services have been replaced by computer systems, anti-virus programs and firewalls. Using fiber optics some black-hat can reach much further, penetrate the structure of the organization incomparably deeper, causing damage many times greater than that occurred in the past.

There are so many threats that it is impossible to list them, every day new forms of attack and previously unknown ways of phishing information and form of stealing money are invented. Initially, sets of rules were created to familiarize employees with dangers.

They focused on the protection of confidential copies and files, on ways of creating access passwords and forms of handling information. In a relatively short time, however, it turned out that the digitized economy requires systematic treatment. The concept of security management in the digital era has emerged; it is systematized and focused on clearly identified areas. The security management in digitalized world includes such areas as: data management, process and work-flow automation, advanced decision-making automation, infrastructure management, intelligent interfaces, management of the external IT ecosystem and management of employee skills and organizational culture. Continuous improvement in the management of these areas will certainly not eliminate threats, but will significantly improve security, which is contemporary „to be or not to be" for any organization.
Key words: digital era, security, cyber crime, management, data protection

Sicherheitsmanagement im digitalen Zeitalter Zusammenfassung

Das digitale Zeitalter schuf neue Eingänge in die Unternehmen und Ämter durch Beschleunigung des Informationsaustauschs und Wechsel der Dokumentationsabläufe. Zugang in die Tiefe der Organisation bietet nicht mehr eine Glaseingangstür sondern das Internet. Das Sicherheitspersonal wurde durch die computergestützten Systeme zum Schutz von Informationen, Antivirenprogramme und Firewalls ersetzt. Über die Glasfaserleitungen kann man wesentlich weiter vordringen, unvergleichbar tiefer die Organisationsstrukturen durchdringen und viel schlimmer schädigen, als die „klassischen" Verbrecher schädigen könnten.

Es gibt so viele Gefahren, dass unmöglich ist alle zu nennen und jeden Tag entstehen neue Angriffsformen und früher nicht bekannte Methoden, wie Informationen zu ergattern und Geld zu erpressen. Anfänglich wurden Grundregeln aufgestellt, mit denen sich die Mitarbeiter vertraut machen sollten. Dies betraf den Schutz von Kopien und vertraulichen Dateien, Methoden der Erstellung der Zugangscodes, Behandlung von Informationen. In kurzer Zeit zeigte sich aber, dass der Schutz vor der Cyberkriminalität eine Systembehandlung erfordert. Es tauchte das Phänomen des Sicherheitsmanagements im digitalen Zeitalter auf – dieses Problem wurde systematisiert und auf klar gegliederte Gebiete konzentriert. Es umfasst: Datenverwaltung, Informationsflussverwaltung, automatisierte Entscheidungen, Verwaltung der Infrastruktur, intelligente Schnittstellen, Verwaltung des äußeren „IT-Ökosystems" und Verwaltung der Fähigkeiten der Mitarbeiter und der Organisationskultur. Die Konzentration auf diese Gebiete behebt nicht die Risiken, aber verbessert wesentlich die Sicherheit, von der oft das Fortbestehen der Organisation abhängt.
Schlüsselwörter: das digitale Zeitalter, Sicherheit, Cyberkriminalität, Sicherheitsmanagement, Datenschutz

Управление безопасностью в эре цифровых технологий Резюме

Цифровая или информационная эра, благодаря ускорению обмену информацией и изменениям форм документооборота, создала новые возможности доступа к предприятиям и государственным учреждениям. Сегодня, не стеклянная

входная дверь, а интернет соединения, дают доступ к организации. Сотрудников службы охраны заместили компьютерные системы информационной безопасности, антивирусные программы и файрволы. Оптическими волокнами можно проникнуть гораздо дальше, проникнуть в структуры организации глубже и нанести ущерб, во много раз превышающий тот, который могли причинить «классические» преступники.

Существует так много угроз, что невозможно их всех перечислить. Ежедневно возникают их новые формы, ранее неизвестные способы хищения информации и денег. Изначально, создавались правила и инструкции, с которыми должны были ознакомиться сотрудники. Эти правила касались защиты файлов, конфиденциальных файлов, способов создания паролей доступа, обработки информации. Однако, за относительно короткий промежуток времени выяснилось, что защита от киберпреступности требует системного подхода. Появилась концепция управления безопасностью в эру цифровых технологий – эта проблема была систематизирована и сосредоточивается на четко выделенных областях. Концепция охватывает следующие области и процессы: управление данными, управление информационными потоками, автоматизация принятия решений, управление инфраструктурой, использование интеллектуальных интерфейсов, управление внешней информационной «экосистемой», управление навыками сотрудников и организационной культурой. Безусловно, концентрация внимания на вышеуказанных областях не устранит угрозы, но значительно повысит безопасность, от которой часто зависит дальнейшее существование организации, предприятия, учреждения.

Ключевые слова: цифровая (информационная) эра, безопасность, киберпреступность, управление безопасностью, защита данных