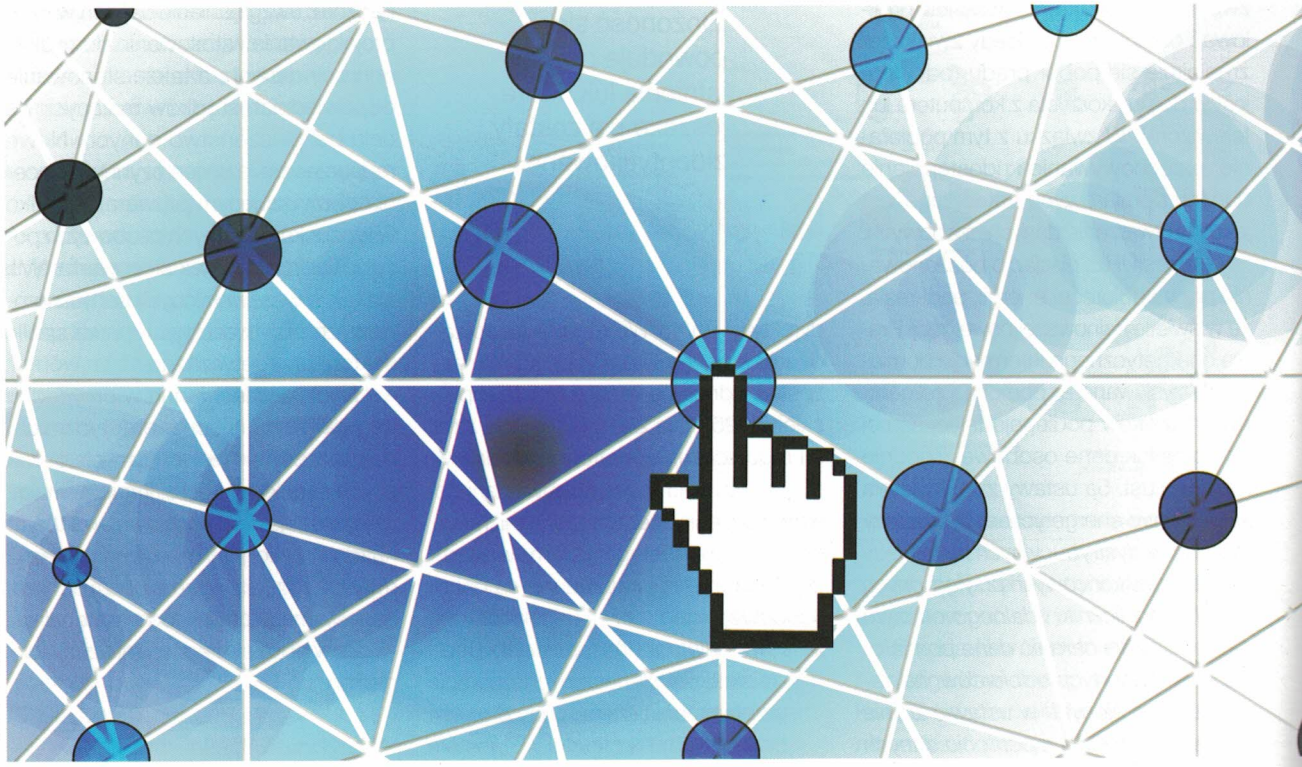
Tadeusz Szulc, ekspert IT, członek Rady Programowej Wydawnictwa „Nowa Energia"

Niebezpiecznie bezpieczni

Na większości internetowych stron dużych banków, firm ubezpieczeniowych i spółek znajdziemy mniej więcej taką informację: „Działamy w oparciu o System Zarządzania Bezpieczeństwem Informacji zgodny z wymaganiami normy ISO/IEC 27001:2013 „Technika informatyczna - Techniki bezpieczeństwa - Systemy zarządzania bezpieczeństwem informacji - Wymagania", co potwierdza uzyskany Certyfikat."



Fot. PIXABAY.COM

Tej treści informacja uspokaja i najczęściej bezrefleksyjnie ufamy, że nasze oszczędności zdeponowane na kontach bankowych są bezpieczne i dalecy jesteśmy od lektury „odpowiedzialności kontraktowej stron podczas korzystania z elektronicznych instrumentów płatniczych".

Wprawdzie wsiadając na prom czy do samolotu widzimy, że właściwe służby podejmują szereg działań mających na celu przeciwdziałanie zidentyfikowanym i potencjalnym zagrożeniom, ale zazwyczaj odbieramy je jako przesadzone i nadmiernie dla nas uciążliwe.

Również z dużą rezerwą i dystansem podchodzimy do stwierdzeń, że „świadome korzystanie z Internetu przez obywateli staje się wymogiem współczesnych czasów" i z ciekawością czytamy o działaniach pentesterów próbujących na zlecenie legalnie włamać się do różnych systemów informatycznych. Urzekają, ale i drażnią zarazem, nas filmy o hakerach, chociaż część osób dostrzega w nich intelektualne, podskórne treści.

Szybko też zapominamy o ostrzeżeniach policyjnych ekspertów mówiących: *Cyberprzestępczości jest najszybciej rozwijającą się przestępczością na całym świecie.*

Dzisiaj młodzi ludzie kończący szkołę podstawową wiedzą jak stworzyć wirusa i wcale nie jest wymagany od nich specjalistyczny zasób wiadomości. W Internecie dostępnych jest wiele generatorów wirusów, których obsługiwanie polega na wyborze odpowiednich funkcji z menu.

Czy zastanawiamy się nad bezpieczeństwem dostępu do zasobów firmowych i wykorzystania przenośnych urządzeń poza swoją firmą? Często, niestety nie, ale zdegustowani jesteśmy jak nam komunikują: „Bezpieczeństwo wymaga ograniczeń. Bezpieczeństwo bywa uciążliwe i trzeba się do tego przyzwyczaić."

Na przestrzeni lat zagadnienia dotyczące bezpieczeństwa ewoluowały i... niestety dzisiaj żyjemy w ciągłym poczuciu niepewności i zagrożenia, a rzeczy dotychczas stałe, dające oparcie, okazały się kruche. Nasze bezpieczeństwo jak to określił jeden z wybitnych ekspertów prognozowania i badania trendów „jest zanurzone jest w świecie nieustannych zagrożeń, i to często zwielokrotnionych".

Klika przykładów opisujących, co się stało, gdy zlekceważono zasady bezpieczeństwa:

- naukowcy firmy DuPont skopiowali 22 000 poufnych dokumentów przed podjęciem pracy u konkurencji;
- z firmy SONY wykradziono dane 77 mln użytkowników PlayStation Network;
- z firmy TJX's „wyciekły" dane warte 1 000 000 000 $;
- grupa bankowa Citigroup straciła nośniki z danymi 3,9 mln klientów podczas transportu przez firmę UPS;
- PenDrive z tajnymi danymi NATO znaleziono w bibliotece w Sztokholmie.

> Cyberprzestępczości jest najszybciej rozwijającą się przestępczością na całym świecie

Trzeba docenić otwartość wyżej wymienionych firm na ujawnienie tego typu informacji, bowiem zazwyczaj z różnych powodów niechętnie dzielą się one informacjami o takich problemach. To jeden z większych problemów związanych z walką z cyberprzestępcami. Panuje dosyć powszechna opinia, że dzielenie się informacjami o cyberatakach mogłoby być jednym z elementów ochrony.

A co u nas?

Na początku 2015 r. została opublikowana Doktryna cyberbezpieczeństwa Rzeczypospolitej Polskiej. Określa ona strategiczne kierunki działań dla zapewnienia bezpieczeństwa Rzeczypospolitej Polskiej w cyberprzestrzeni.

Na dniach ukazała się informacja Najwyższej Izby Kontroli z przeprowadzonych w latach 2015 i 2016 kontroli sprawdzenie prawidłowości zabezpieczenia obiektów infrastruktury krytycznej (IK) istotnych dla funkcjonowania państwa.

W interesującym nas obszarze, znajdziemy w raporcie stwierdzenie:

(...) wystąpiły przypadki nierealizowania przez skontrolowane podmioty niektórych rekomendacji audytu sieci informatycznych działających na potrzeby obiektów infrastruktury krytycznej, nieopracowania kompleksowych regulacji wewnętrznych dotyczących bezpieczeństwa przemysłowego systemu teleinformatycznego, czy też niezobowiązywania wykonawców do zachowania poufności uzyskanych informacji, mimo że podczas realizacji zadań mieli dostęp do kluczowych systemów służących do sterowania IK (...)

Myślę, że ta informacja nie wymaga żadnego komentarza, chociaż część osób powinna szybko zapoznać z tym raportem (jest dostępny pod: https://www.nik.gov.pl/aktualnosci/nik-o-bezpieczenstwie-obiektow-infrastruktury-krytycznej.html).

Jak z powyższego wynika: zagrożone są systemy ekonomiczne, porządek polityczny, pokój i stabilność na świecie. Coraz trudniej jest nam wyobrazić sobie bezpieczną przyszłość: zarówno odleglejszą, jak i całkiem bliską.

Dzisiejszy czas często jest nazywany Internetem przedmiotów (IoT), Przemysłem 4.0 czy wiekiem maszyn cyfrowych. Dla wszystkich oczywiste jest, że wkraczamy w nową rewolucję przemysłową. Wpływ nowej technologii oznacza komputeryzację wszystkiego, co oznacza, że zagrożenia też się upowszechniły, a prawdopodobieństwo cyberataku na np. media elektroniczne, kanały komunikacji, systemy informatyczne czy energetykę zdecydowanie wzrosło. Również rośnie ilość

hakerów, informatyków-anarchistów oraz przestępców działających w cyberprzestrzeni. Wszystko to dzieje się w ramach działań, w wymiarze międzynarodowym określanych jako wojna informacyjna z elementami cyberwywiadu, cyberagentury, nowego typu propagandy oraz manipulacji informacją *(trolling)*. Jak poważne są to zagrożenia, nich świadczy choćby fakt wprowadzenia w związku ze Światowymi Dniami Młodzieży ogólnego stopnia alarmowego ALFA oraz stopnia alarmowego BRAVO-CRP dla cyberprzestrzeni.

W tym miejscu warto również zaapelować o ponowną lekturę lub wręcz zapoznanie się z raportem, z ćwiczeń dotyczących ochrony infrastruktury krytycznej przed atakiem z cyberprzestrzeni - Cyber-EXE Polska 2012. Dla przypomnienia: ćwiczenia te zostały przeprowadzone we współpracy z Europejską Agencją ds. Bezpieczeństwa Sieci i Informacji (ENISA), powołaną przez Parlament Europejski i Radę do wsparcia krajów członkowskich w działaniach zwiększających bezpieczeństwo w Internecie.

Bezpieczeństwo jest jednym z obszarów aktywności, o który niezmiernie dbają markowe firmy, budując swój wizerunek. To dzisiaj obowiązek, bowiem celem cyberataków jest najczęściej uzyskanie korzyści ekonomicznych, rynkowych, politycznych lub społecznych.

Wiele z nich utworzyło w swoich organizacjach stanowiska Administratorów Bezpieczeństwa Informacji (ABI). Inni poszli dalej tworząc Centra Zarządzania Kryzysowego.

Wespół z tymi działaniami opracowano i wdrożono szereg polityk i procedur podnoszących bezpieczeństwo przed cybertakiem oraz - co jest niezmiernie ważne - opracowano metody przywracania funkcjonowania po nieautoryzowanym dostępie do danych i systemów.

Dzisiaj już nikt nie kwestionuje potrzeby oddzielanie systemów sterowania i automatyki przemysłowej od innych sieci. Ten rozdział znakomicie zabezpiecza systemy przemysłowe przed poleceniami i informacjami napływającymi z sieci firmowej.

Zapory firewall, weryfikacja tożsamości, autoryzacja dostępu, sieci VPN (IPsec) i oprogramowanie antywirusowe blokujące dostęp osobom bez uprawnień to już dzisiejsza codzienność.

Aktualnie prace zabezpieczeniowe szeregu firm koncentrują się nad ograniczeniem zasięgu potencjalnych naruszeń do jednego segmentu sieci. Odbywa się to przy pomocy przełączników sieciowych i sieci VLAN dzielących sieć na kilka podsieci i ograniczających wymianę danych pomiędzy nimi. Pomaga to ograniczyć negatywne skutki ataku złośliwego oprogramowania do jednego segmentu, redukując straty w całej sieci.

> Dzisiaj młodzi ludzie kończący szkołę podstawową wiedzą jak stworzyć wirusa i wcale nie jest wymagany od nich specjalistyczny zasób wiadomości. W Internecie dostępnych jest wiele generatorów wirusów, których obsługiwanie polega na wyborze odpowiednich funkcji z menu

Prawda, że to zdumiewające ile pracy może wymagać zapewnienie bezpieczeństwa. Tym bardziej zdumiewające, że - gdy uda się o nie zadbać naprawdę dobrze - beneficjenci tego prawdopodobnie w ogóle nie zauważą.

Ale prawda, jest również zgoła inna

Ogromna ilość danych często uniemożliwia skuteczną analizę zagrożeń. Zgadzają się co do tego najwięksi dostawcy rozwiązań bezpieczeństwa (m.in. ThreatQuotient, TruSTAR, BrightPoint, Webroot, Norse i Adollom).

W stosunku do zeszłego roku liczba ataków na świecie wzrosła o 38% a średni czas uzyskania nieautoryzowanego dostępu do systemów i danych to 4 godziny.

Tylko w Polsce średnio rocznie na każdą firmę przypadało aż 126 cyberataków.

Poszczególne Państwa nie zawsze dysponują wystarczającym potencjałem działań zapobiegającym zagrożeniom. To konsekwencja poziomu ich rozwoju, funkcjonowania instytucji politycznych i świadomości mieszkańców.

W Polsce, po kilku latach nieśmiałych apeli o podjęcie pilnych prac nad tym zagadnieniem, nareszcie temat ten doczekał się zaawansowanych i merytorycznych dyskusji o konieczność przeprowadzenia szeregu zmian organizacyjnych, reform instytucjonalnych i prawnych.

Poczyniono szereg większych inwestycji. Podniesiono kompetencje szeregu osób.

To są bardzo potrzebne działania, bo skalę uzależnienia świata od Internetu obrazuje ilość podłączonych do niego urządzeń, którą szacuje się na 30 mld w 2020 r.

Jak podaje Forbes, w 2015 rynek cyberbezpieczeństwa był wyceniany na 75 mld $. Przewiduje się, że w 2020 jego wartość wyniesie 170 mld $.

Coraz powszechniejsze staje się również przekonanie, że wiedza na temat bezpieczeństwa powinna być dystrybuowana szeroko, a nie być zarezerwowana wyłącznie dla wąskiego grona firm, zwłaszcza technologicznych.

Myślę, że powołanie niedawno Narodowego Centrum Cyberbezpieczeństwa (NCC) to, wprawdzie spóźniony, ale właściwy krok, w szeregu zadań ja-

kie są do wykonania w zakresie cyberbezpieczeństwa w Polsce. NCC działa w trybie 24/7 przez 365 dni w roku i ma za zadanie wczesne ostrzeganie i szybkie reagowanie w razie ewentualnych ataków jak również koordynowanie działań i wymianę informacji.

Odpowiadając na zapotrzebowanie rynku, kilka uczelni w Polsce zdecydowało się wprowadzić do swoich wolumenów nauczania podyplomowe studia zarządzania cyberbezpieczeństwem. Umożliwiają one zapoznanie się i dogłębne zrozumienie zagrożeń cyfrowych. Zajęcia na tych studiach prowadzone są przez wybitnych praktyków z wiodących firm branży bezpieczeństwa teleinformatycznego, zarządzania ryzykiem, jak i pracowników akademickich mających praktyczne doświadczenie w biznesie.

Bardzo ciekawą inicjatywą jest projekt Cyfrowobezpieczni.pl - Bezpieczna Szkoła Cyfrowa. Jego autorzy chcą skutecznie od-

> Panuje dosyć powszechna opinia, że dzielenie się informacjami o cyberatakach mogłoby być jednym z elementów ochrony

powiedzieć na problemy i wyzwania związane z bezpiecznym korzystaniem z zasobów cyberprzestrzeni w polskich szkołach.

Jednym z celów programu jest wzbogacenie wiedzy i świadomości uczniów, ale także nauczycieli i rodziców na temat możliwych zagrożeń i ryzyka związanego z korzystaniem z Internetu i nowoczesnych narzędzi cyfrowych.

W lipcu tego roku Parlament Europejski przyjął dyrektywę o bezpieczeństwie sieci i informacji (tzw. dyrektywę NIS).

NIS to pierwsze unijne prawo dotyczące bezpieczeństwa.

Realizowanie tej dyrektywy ma przede wszystkim zapewnić, że cyfrowa infrastruktura dla usług o znaczeniu krytycznym będzie odpowiednio zabezpieczona przed cyberatakami.

Dotyczy ona, przede wszystkim, takich sektorów jak: energetyka, transport, ochrona zdrowia, bankowość i zaopatrzenie w wodę pitną.

Internet wpłynął na funkcjonowanie wszystkich jego użytkowników. Rodzaje i skala zarówno korzyści, jak również zagrożeń związanych z funkcjonowaniem w cyberprzestrzeni różnią się w zależności od użytkownika sieci, dlatego bezpieczeństwo z jej korzystania należy rozpatrywać na poziomie jednostki, organizacji oraz państwa.

Skoro są tak wielkie zagrożenia, to jak się przed tymi zagrożeniami zabezpieczyć?

Można i trzeba!

Posłużę się tutaj bliskim mi przykładem firmy Xerox®, w której od dwóch lat pracuję.

Firma Xerox® wyposażyła większość swoich urządzeń w najbardziej kompletny zestaw funkcji, technologii i rozwiązań dostarczanych przez liderów branży zabezpieczeń, które chronią informacje o krytycznym znaczeniu przed wszelkimi potencjalnymi lukami w zabezpieczeniach.

Systemy wielofunkcyjne Xerox® ConnectKey™ zawierają zintegrowaną technologię McAfee®, dzięki czemu powstała pierwsza w branży linia systemów wielofunkcyjnych, które same zabezpieczają się przed potencjalnymi zagrożeniami zewnętrznymi. Technologia białych list McAfee zapewnia, że w urządzeniu mogą być uruchamiane tylko bezpieczne, wcześniej zatwierdzone pliki systemowe, do minimum ograniczając konieczność ręcznego aktualizowania oprogramowania zabezpieczającego przed nowymi zagrożeniami dla bezpieczeństwa. Ponadto płynna integracja z zestawem narzędzi Xerox® MPS oraz McAfee ePolicy (ePO) umożliwia łatwe śledzenie i monitorowanie. Ponadto automatyczna integracja Cisco TrustSec Identity Services Engine (ISE) zapewnia kompleksową widoczność wszystkich punktów dostępu do wielofunkcyjnych systemów ConnectKey, aby wdrażać zarządzane przez dział informatyczny scentralizowane zasady bezpieczeństwa i zgodność.

Rozwiązania Xerox® umożliwiają również:

- zabezpieczenie wszystkich wrażliwych danych stosując szyfrowane pliki PDF podczas skanowania,
- pełne szyfrowanie twardego dysku zgodne z normą 140-2 256-bit AES FIPS oraz nadpisywanie plików z procesem trzykrotnego zamazywania, zapewniającego całkowite usunięcie wszystkich fragmentów danych,
- dostęp do urządzenia tylko i wyłącznie uwierzytelnionym użytkownikom, stosując uprawnienia użytkownika Xerox®, uwierzytelnianie sieciowe, filtrowanie IP, karty inteligentne i logowanie oparte o role, i dające dostęp tylko do określonych funkcji,
- monitorowanie punktów ochrony pod kątem nowych luk w zabezpieczeniach i, w razie potrzeby, dostarczanie poprawek, zapewniające aktualność zabezpieczeń sprzętu oraz bezpieczeństwo danych.

> „(...) wkraczamy w nową rewolucję przemysłową. Wpływ nowej technologii oznacza komputeryzację wszystkiego, co oznacza, że zagrożenia też się upowszechniły (...)

Urządzenia firmy Xerox® są zgodne z najnowszymi normami bezpieczeństwa różnych branż, w tym rządowymi, finansowymi i medycznymi. Należą do nich Common Criteria, HIPAA, Data Protection Act (Ustawa o ochronie danych), COBIT i inne.

To są rozwiązania z najwyższej półki, jedyne i wyjątkowe, ale... w procesach przetargowych zwalczane przez konkurencję powołującą się na „utratę możliwości uzyskania zamówienia lub ubiegania się o udzielenie zamówienia z uwagi na brak możliwości złożenia oferty równoważnej".

Quo vadis? Obyśmy nie zagubili się we współczesnym chaosie przetargowym. Bezpieczeństwo jest ważniejsze, a poza logiką jest tylko absurd.

Wykorzystujmy to, co dziś jest aktualne, bo rozwiązania sprzed kilku lat pachną dostojną przeszłością i u hakerów wywołują tylko uśmiech politowania.

Nie chodzi nawet o to, że w ten sposób banalizujemy pojęcie bezpieczeństwa i pokazujemy, że totalnie nie rozumiemy tego słowa. Jest to kompletne niezrozumienie oczekiwań klienta.

Żyjemy dziś w ciągłym poczuciu niepewności. Rzeczy dotychczas stałe, dające oparcie, okazały się kruche. Sięgamy więc po dopracowane w każdym szczególe sposoby radzenia sobie z tą niepewnością, przede wszystkim po rozwiązania kompletne, a nie fragmentaryczne. Niczego nie uśredniamy.

Nie ma nic gorszego jak przekonanie, że się jest bezpiecznym nie będąc nim.

Moja najstarsza wnuczka nazwała ten stan „niebezpiecznie bezpiecznym". W pełni się z nią zgadzam. □

Fot. PIXABAY.COM