Tadeusz Szulc, Ekspert IT, Członek Rady Programowej Wydawnictwa „Nowa Energia”

Zmierzyć się z cyberzagrożeniem

Niedawno postawiono mi pytania:
Jak bardzo nasza cywilizacja zmieni się pod wpływem nieustannego i dynamicznego rozkwitu cyfrowych zagrożeń?
Jak zagrożenia te wpłyną na jakość otoczenia, w którym żyjemy?
Jak będzie wyglądał przebieg kolejnych wydarzeń społecznych, politycznych i kulturalnych w obliczu zagrożenia cyberatakami?

Dzisiaj wiele osób mówi, że sposób działania i zarządzania cyberbezpieczeństwem stanowi o przetrwaniu. Oczywiście kluczową kompetencją w tych działaniach jest rozróżnianie, co jest ważne, a co nie jest. Jednak zawsze wkrada się tutaj ryzyko oceny, na ile istotne jest określone wydarzenie. O tym, jak bardzo sprawa jest poważna, może świadczyć na przykład fakt zabezpieczania się za pomocą najnowszych metod automatycznego rozpoznawania i analizy danych biometrycznych. Źródłem tych danych są pomiary charakterystyk fizycznych człowieka, obserwacje jego zachowań oraz monitorowanie procesów związanych z jego funkcjonowaniem.

Prowadzone są, między innymi, bardzo ciekawe badania i doświadczenia związane z możliwością np. przejęcia kontroli nad planem lotu i różnymi opcjami komputerów w samolocie. W skrócie: aby taki atak hakerski się udał, należałoby wprowadzić fałszywe parametry do komputerów sterujących, wymusić wykonanie niespodziewanych manew-

rów, a potem spowodować zamieszanie w kokpicie. Na szczęście, lotnictwo nigdy nie polega na jednej metodzie zabezpieczeń, choćby najsprawniejszej. Dlatego w razie próby wprowadzenia zmian do planu lotu, pilot takiej zmiany po prostu nie zatwierdzi. Gdyby jednak udało się włamywaczowi zmienić kierunek, prędkość lub wysokość, inne systemy podniosą alarm. Do tego dochodzi zachowanie pilota, wyuczone przez całe lata szkoleń i praktyki.

Aktualnie sporą uwagę budzi RODO (Rozporządzenie o Ochronie Danych Osobowych) i Dyrektywa NIS (obowiązki dla operatorów usług kluczowych na rzecz wysokiego poziomu bezpieczeństwa sieci i systemów informatycznych). Odbywają się liczne konferencji z udziałem przedstawiciel uczelni, firm audytorskich i informatycznych oraz dozoru technicznego, którzy biorą lub brali udział w licznych audytach bezpieczeństwa teleinformatycznego oraz w budowie lub modyfikacji systemów bezpieczeństwa dużych organizacji, zarówno komercyjnych jak i państwowych.

Jest oczywiste, że aby być w dostateczny sposób zabezpieczonym trzeba podjąć określone działania. Podkreślam słowo „dostateczny" - w tej dziedzinie przymiotników „dobry" i „bardzo dobry" się nie używa.

Na jednej z konferencji przedstawiciel koncernu naftowego tak określił bieżące i perspektywiczne działania (rozwiązania) jakie podejmuje i podejmować się będzie w tym przedsiębiorstwie:

1. Budowa SOC (Security Operations Center) – perspektywa CERT (instytucja, która czuwa nad cyberbezpieczeństwem Polski).
2. Współpraca z NASK (Naukowa i Akademicka Sieć Komputerowa; podlega Ministerstwu Cyfryzacji, instytucja badawcza).
3. Współpraca z www.cert.gov.pl (pełni rolę głównego zespołu CERT w obszarze administracji rządowej i obszarze cywilnym).
4. Współpraca z RCB (Rządowe Centrum Bezpieczeństwa).
5. Współpraca z ICCSS (International Centre for Chemical Safety and Security) – audyt stanu bezpieczeństwa w obszarze cyberbezpieczeństwa (narzędzie CSET).

Cyberbezpieczeństwo jest ściśle związane z procesem starzenia się rozwiązań zabezpieczających. To „starzenie się" może mieć różne tempo. Wyróżnić możemy: starzenie normalne, przyspieszone i przedwczesne. Prawdą jest, że proces ten, jeżeli jest niekontrolowany, może być poważnym zagrożeniem i doprowadzić do wystąpienia szeregu zmian strukturalnych i czynnościowych, upośledzających funkcjonowanie przedsiębiorstwa. Często refleksja nad faktem, że należy zawczasu myśleć o modernizacji i modyfikacji rozwiązań zabezpieczających, przychodzi zbyt późno.

> Cyberbezpieczeństwo jest ściśle związane z procesem starzenia się rozwiązań zabezpieczających

Przykładów takich sytuacji jest wiele. Ograniczę się tylko do dwóch:

1. Czerwiec 2017: przez złośliwe oprogramowanie największy na świecie operator morskiego transportu kontenerowego musiał ograniczyć działalność, zmuszony został również zawiesić funkcjonowanie systemu do zarządzania statkami. Przez kilka dni niektóre załogi nie dostawały nowych zleceń. Maersk twierdzi, że choć atak wirusa spowodował poważne straty finansowe, nie doszło do wycieku danych.
2. Maj 2017: co najmniej 40 organizacji regionalnych działających w ramach służby zdrowia, w tym szpitale w Londynie, zostało dotkniętych atakiem uniemożliwiającym korzystanie z sieci informatycznych i telefonicznych. Brytyjska premier Theresa May powiedziała, że cyberatak na systemy informatyczne brytyjskiej służby zdrowia (NHS) jest „częścią szerszego, międzynarodowego ataku". Jak podkreśliła, nie ma dowodów na to, że dane pacjentów ucierpiały w wyniku incydentu.

Dla wielu przedsiębiorstw owo „starzenie się" zazwyczaj następuje w wyniku różnych przyczyn zewnętrznych i nie jest poprzedzane żadnymi widocznymi objawami.

Aby przetrwać w warunkach dynamicznego otoczenia zarządzający organizacjami muszą nadążać za zmieniającym się rynkiem i oczekiwaniami nabywców. Przedsiębiorstwa, które pragną się rozwijać i zająć mocną pozycję na rynku muszą antycypować nadchodzące zmiany i reagować na nie szybciej niż konkurencja. Tworzenie i utrzymywanie połączeń infrastruktury przedsiębiorstw jest niezbędnym elementem procesu ustawicznego ich rozwoju. Jest to jednak cecha krytyczna zagrożona atakami hakerskimi. Tym bardziej, że należy zabezpieczyć się zarówno przed szkodą lub stratą powstałą w wyniku zaistnienia sytuacji przypadkowej, będącej efektem niewiedzy, zaniedbania lub zlekceważenia pewnych norm i procedur jaki i przed szkodami powstałymi przez działania hakerów.

Wydaje się więc naturalne, że konieczne jest łączne i całościowe zbadanie podatności infrastruktury na istniejące zagrożenia. Badanie takie można przeprowadzić np. za pomocą programu CSET. Jest to program służący do badania podatności na cyberatak, opiera się na bazie ok. 2.000 pytań,

które zostały sformułowane w oparciu o wymagania poszczególnych norm NIST. Normy NIST (National Institute of Standards and Technology) obowiązują w USA (w Europie odpowiednikiem norm NIST są normy ISO) i są w wielu elementach bardziej rygorystyczne niż wymagania norm ISO. Pytania są podzielone na 28 kategorii i dotyczą, między innymi, zarządzaniu konfiguracją, sposobu reagowania na incydenty, kontroli dostępu do danych, integralności stosowanych systemów czy szkolenia pracowników. CSET jest więc bazą wiedzy na temat sposobu zabezpieczenia przedsiębiorstwa przed cyberatakami. Główną wartością programu jest również jego pomoc w budowania świadomości zarówno na poziomie pracowników technicznych, jak i na poziomie zarządu. Program po analizie odpowiedzi na postawione pytania generuje raport o największych zagrożeniach oraz wskazuje te obszary poprawy bezpieczeństwa, które mogą być najszybciej naprawione.

Warto mieć taki raport. Szczególnie, że dziś wielu pyta:

- Czy Twój biznes wykorzystuje technologie cyfrowe?
- Czy Twoja marka przeniosła się już do świata usług cyfrowych, a oferowany przez nią produkt jest wyjątkowy?
- Czy Twoja firma wyróżnia się w branży dzięki cyfrowym ekosystemom i realizuje strategię tworzenia nowych wartości, dopasowując się jednocześnie do indywidualnych potrzeb klienta?

Jednak efekty cyfrowej transformacji biznesu trzeba w należyty sposób zabezpieczyć. Obowiązkowo, bowiem tylko w okresie pisania tego tekstu bez trudu można było znaleźć informację o kolejnym zmasowanym ataku hakerskim na systemy informatyczne Ukrainy, ostrzeżeniach dwóch banków (PKO BP i mBank) przed atakami na osoby, które korzystają z bankowości elektronicznej oraz falą fałszywych e-maili od osób podszywających się pod Pocztę Polską zawierających złośliwe oprogramowanie lub link do przygotowanej przez hakerów strony internetowej.

25 maja 2018 roku zmieni się system prawny, dotyczący ochrony danych osobowych. Nowe przepisy (RODO) będą wzmacniać prawa osób, których dane są zbierane, natomiast na przedsiębiorców i inne podmioty przetwarzające dane będą nałożone nowe obowiązki. Każdy administrator danych zobowiązany jest do tego, by dane osobowe przetwarzał z poszanowaniem podstawowych zasad. Rozporządzenie tak definiuje zasadę integralności i poufności: „Dane osobowe muszą być przetwarzane w sposób zapewniający odpowiednie bezpieczeństwo danych osobowych, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych".

> Dzisiaj już wiadomo, że od 25 maja 2018 r. kary dla przedsiębiorców za naruszenie ochrony danych osobowych będą znacznie bardziej dotkliwe niż obecnie i będą mogły sięgnąć 20 mln euro lub 4 proc. światowego obrotu firmy

Oznacza to, że każdy, kto przetwarza dane osobowe, musi odpowiednio je zabezpieczyć, tak by uniemożliwić ich nieuprawnione udostępnienie. Poza uchwaleniem nowej ustawy o ochronie danych osobowych, konieczne jest także dokonanie licznych zmian w innych ponad 130 ustawach zapewniających dostosowanie krajowego porządku prawnego do nowych norm prawnych.

Na dzień dzisiejszy stan jest taki:

- RODO zacznie być aktem bezpośrednio stosowanym od dnia 25 maja 2018 r. (data wejścia w życie unijnych przepisów),
- Ministerstwo Cyfryzacji (organ właściwy do przygotowania nowej regulacji prawnej) ogłosiło projekt nowej ustawy, do którego zgłoszono szereg uwag.

Dzisiaj już wiadomo, że od 25 maja 2018 r. kary dla przedsiębiorców za naruszenie ochrony danych osobowych będą znacznie bardziej dotkliwe niż obecnie i będą mogły sięgnąć 20 mln euro lub 4% światowego obrotu firmy.

Każda instytucja będzie musiała wdrożyć odpowiednie procedury bezpieczeństwa i zbudować system raportowania. Przepisy RODO zakładają, że funkcję administratora bezpieczeństwa informacji (ABI) w firmach przejmie inspektor ochrony danych (IOD). Do tej pory, państwami w których już uchwalono przepisy wdrażające rozporządzenie są jedynie Niemcy i Austria.

Funkcjonowanie przedsiębiorstwa wymaga oceny w aspekcie jego stabilności i bezpieczeństwa. Coraz częściej najważniejszym kryterium tej oceny staje się adekwatność posiadanych przez nie zabezpieczeń.

Wszelkie działania uwzględniające RODO, NIS i cyberbezpieczeństwo były, są i będą próbą kompleksowego rozwiązania kwestii bezpieczeństwa z uwzględnieniem historycznych, prawnych i instytucjonalnych uwarunkowań, a także problemów, które wpisują się aktualnie w społeczną przestrzeń.

Likwidacja różnic w rozwoju poziomu zabezpieczeń staje się ogólnoświatowym priorytetem.

Musimy zmierzyć się z tym zagrożeniem. □