ALERT BIZNESOWY

9

Dominika Bettman
prof. dr hab. Andrzej Jacek Blikle
dr Henryka Bochniarz
Tomasz Brzostowski
Tomasz Budziak
Wojciech Eichelberger
Joanna Erdman
Jarosław Grzesiak
prof. dr hab. Jerzy Hausner
dr Ewa Łabno-Falęcka
prof. dr hab. Krzysztof Obłój
Przemysław Powalacz
Piotr Voelkel
Mateusz Zmyślony

gap.

open eyes economy summit

Cyber-bezpieczeństwo

8 czerwca 2020 r. hakerzy zaatakowali system IT międzynarodowej korporacji Avon. Jego podsystemy jeden po drugim przestały działać. Mówimy o gigantycznej korporacji o obrotach powyżej 5 mld dolarów, dla której system IT jest fundamentalnie ważny dla realizacji jakichkolwiek transakcji. Firma sama nie wie, kiedy i jak jej systemy zostały zainfekowane oraz jakie są tego konsekwencje.

Prawie zawsze w tej sytuacji firmy mają ten sam komunikat: „*The Company is evaluating the extent of the incident and working diligently to mitigate the effects, applying all efforts to normalize operations*”. Nic z niego nie wynika poza jednym: nie ma bezpiecznych systemów IT. Są tylko lepiej lub gorzej chronione. Oznacza to, że strategicznie firma musi stale stawiać sobie dwa strategiczne pytania: (1) **dlaczego systemy powinny być jak najlepiej zabezpieczone,** 2) **jak zapewnić to bezpieczeństwo**.

Odpowiedź na pytanie „dlaczego?” jest prosta: Dane są fragmentem tożsamości firmy i jej pracowników, dostawców, klientów. Ograniczony dostęp do nich jest składową kontraktu rynkowego, który firma zawiera ze swoimi interesariuszami. Jeśli ten kontrakt zostaje złamany, cierpi reputacja firmy i zaufanie do niej zanika.

Odpowiedź na pytanie „jak?” jest znacznie bardziej skomplikowana i natury technicznej. Najprościej można powiedzieć, że wymaga to stałego testowania systemu, łatania jego dziur, staranności wszystkich użytkowników w doborze haseł, kontroli logowania i wylogowywania z systemu oraz dokładnej analizy wszystkich, nawet najsłabszych sygnałów, że coś mogłoby być nie tak. Dodatkowo wskazane są okazjonalne, celowe, profesjonalnie przeprowadzane

próby łamania własnych zabezpieczeń, w celu szukania słabych punktów systemu.

Niebezpieczeństwa związane z upowszechnianiem się produktów szeroko rozumianego przemysłu IT można w głównej mierze podzielić na trzy kategorie:

1. Związane z błędami w systemach informatycznych.

2. Związane z nieumiejętnym posługiwaniem się narzędziami IT przez użytkowników.

3. Związane z działaniem przestępczym, takim jak sabotaż systemów (energetycznych, finansowych, obronnych itp.), kradzieże informacji, pieniędzy i dóbr materialnych (np. ciężarówek wraz z ładunkiem), rozsiewanie dezinformacji itp.

Błędy w systemach IT

Za bezpieczeństwo teleinformatyczne (cyberbezpieczeństwo) odpowiadają również producenci, dostawcy oprogramowania wykorzystywanego przez dany IT. Producenci oprogramowania, broniąc się przez możliwym zarzutem oraz odszkodowaniem spowodowanym błędem w ich programie, z reguły wyłączają swoją odpowiedzialność następującym ustępem w treści licencji:

Producent oprogramowania zwraca uwagę, że w oparciu o bieżący stan techniki, nie jest możliwe wyprodukowanie programu komputerowego w taki sposób, aby bezbłędnie pracował we wszystkich możliwych konfiguracjach. Producent gwarantuje w oparciu o doświadczenie dotychczasowych

użytkowników, że do dnia zawarcia niniejszej umowy nie zna żadnych błędów w przekazywanym programowaniu.

Kuriozalność tej deklaracji polega na tym, że producent gwarantuje, iż nie zna żadnych błędów w przekazywanym programowaniu. Jedyne więc, co jest w stanie zagwarantować użytkownikowi, to że odkrywane w przyszłości błędy będą również dla niego prawdziwą niespodzianką. Domyślnie oznacza to także, że taki stan rzeczy pozwoli producentowi wypuszczać na rynek kolejne, „ulepszone" wersje swojego produktu, co będzie objęte dodatkowo płatnym abonamentem serwisowym.

Jest powszechnie znanym faktem, że użytkownik nabywający aplikację informatyczną musi taki stan rzeczy zaakceptować i to na piśmie przyjmując tzw. „wyłączenia odpowiedzialności" (*disclaimer*) ze strony producenta aplikacji.

Trudno sobie wyobrazić, że producent jakiegokolwiek nieinformatycznego produktu przemysłowego — samochodu, pralki, telewizora czy budynku — mógłby zażądać od swoich klientów zgody na podobne zrzeczenie się swoich praw. Jednakże w przemyśle IT jest to zjawisko praktycznie nie znające wyjątków.

Z reguły w danym systemie informatycznym współpracuje ze sobą wiele programów. Brak gwarancji niezawodności jednego z nich powoduje rozszerzenie braku tej gwarancji na inne programy. W rezultacie nie ma gwarancji producentów, że cały system będzie zawsze działać poprawnie i będzie odporny na nieautoryzowane użytkowanie.

Szybkie lekcje z pandemii

Obserwujemy bezprecedensowy wzrost znaczenia cyfrowych kanałów komunikacji w firmie po-COVID'owej. Firmy w sposób dramatyczny uzależniły się w ostatnich 4 miesiącach od wszelkiego rodzaju aplikacji video-konferencyjnych. Firmy najczęściej korzystają z jednej aplikacji tego rodzaju, nie budując – póki co – alternatywy/ścieżki bezpieczeństwa na wypadek … „awarii". Oczywiście teoretycznie istnieją coraz liczniejsze ogólnodostępne platformy (np. z poziomu przeglądarki internetowej), ale wtedy pod znakiem zapytania staje bezpieczeństwo przekazywanych treści (prowadzanych rozmów, emitowanych prezentacji, etc.) oraz efektywność samego narzędzia (przy kilkuset osobowej firmie jest to już wyzwaniem).

Poza tym narzędzia do zwykłej rozmowy czy konferencji to już zdecydowanie za mało. Firmy muszą coraz częściej sięgać do **narzędzi zdalnej pracy grupowej (twórczej, warsztatowej),** takich jak: Miro, Mural, Whiteboard, Freehand, Mindmeister, Conceptboard, etc.

Ogromna część pracowników firm wciąż pracuje z domu, a sprawne łącze w domu pracownika staje się także problemem pracodawcy. Sprawne tj. odpowiednio szybkie, stabilne, zapewniające możliwość aktywacji połączeń tunelowych/szyfrowanych.

Nie da się już uniknąć permanentnego rozwijania **kompetencji cyfrowych pracowników** – systemowo, w całej organizacji, na każdym niemal stanowisku. Czasy, w którym zadzwonimy po kolegę IT, żeby pokazał jak się włącza coś w jakimś programie odeszły do lamusa.

Zaledwie 25% młodych ludzi w UE określa siebie jako „mających wysoki poziom kompetencji informatycznych", przez co rozumieją, że potrafią

korzystać z wyszukiwarek internetowych, umieszczać wiadomości na forach dyskusyjnych, wysyłać maile „z załącznikami", dokonywać zakupu i wymiany plików muzycznych itp. W tej sytuacji nie dziwi fakt, że aż 46-56% firm we wszystkich sektorach bezskutecznie poszukuje informatyków, którzy zajęliby się ich systemami informatycznymi i ich ochroną przed rozmaitymi zagrożeniami.

Rodzaje ataków hakerskich:

- wysyłanie zainfekowanych informacji, podszywając się pod użytkownika sieci (*spoofing*),
- udawanie osoby lub instytucji godnej zaufania i wyłudzanie danych/pieniędzy (*phishing*),
- tworzenie imitacji strony internetowej, np. banku i w ten sposób uzyskiwanie danych do logowania (*pharming*).
- monitorowanie przepływu danych, takich jak nazwy użytkowników czy hasła (*sniffing*),
- blokada sieci przez zajęcie wszystkich wolnych zasobów serwerów i ataki równocześnie z wielu komputerów (*DDoS*),
- wysyłanie ogromnych ilości danych, co obciąża serwer (*SYN flooding*).

Ataki z wewnątrz (*inside attackers*)

Raport Data Breach Investigation amerykańskiego giganta telekomunikacji Verizon zwraca uwagę na 5 typów tzw. *inside attackers*:

1. Nieostrożny pracownik, który celowo łamie lub obchodzi zasady dopuszczalnego użytkowania systemów teleinformatycznych, np. przez instalowanie nieautoryzowanych aplikacji, wyłączanie oprogramowania zabezpieczającego albo łamanie ustalonych procedur. Działania te często nie są złośliwe, lecz podyktowane brakiem wiedzy lub chęcią uproszczenia pracy.
2. Agent wewnętrzny – osoba mająca dostęp do informacji poufnych, zrekrutowana lub przekupiona z zewnątrz w celu przekazywania danych.
3. Niezadowolony pracownik, który ma dostęp do poufnych informacji i usiłuje zaszkodzić swojej organizacji, niszcząc dane albo zakłócając jej działalność.
4. Złośliwy informator – pracownik z dostępem do danych korporacyjnych, który wykorzystuje nadane mu w systemie uprawnienia dla osobistego zysku. Może być motywowany przez hakerów prowizją od okupu przy okazji ataku albo zainteresowany sprzedażą własności intelektualnej.
5. Beztroska trzecia strona to partner biznesowy, kontrahent narażający firmę na wyciek danych poprzez zaniedbanie lub niewłaściwe użycie danych. Ta kategoria obejmuje również podmioty trzecie, które niewłaściwie zarządzają informacjami, ewentualnie celowo powodują wyciek.

Ochrona przed cyberatakami

Ochrona obejmuje wiele elementów takich jak aktualizacja oprogramowania i systemów operacyjnych, tworzenie silnych haseł i dwuskładnikowego uwierzytelniania (dwie metody weryfikacji), zwracanie uwagi na podejrzaną aktywność, ochrona danych osobowych, używanie szyfrowanej (bezpiecznej) komunikacji internetowej, tworzenie kopii zapasowych plików aż po ochronę domowej i/lub służbowej sieci WiFi.

Zaatakowanie pojedynczego czy nawet grupy poszczególnych urządzeń, nie spowoduje raczej większych szkód, ale poprzez nie może nastąpić atak na centralne systemy teleinformatyczne. Wówczas skutki mogą okazać się bardzo poważne.

Państwo powinno wspomagać obywateli w zabezpieczaniu się oraz obronie przed atakami teleinformatycznymi. W tym celu potrzebne jest Centrum Wspomagania Bezpieczeństwa Teleinformatycznego, które powinno edukować i informować zwykłych użytkowników systemów o aktualnych zagrożeniach oraz sposobach ich unikania, dystrybuować programy zabezpieczające oraz pomagać w odzyskaniu danych i usunięciu skutków ataków.

W USA istnieje procedura prawna umożliwiająca operatorom na żądanie służb państwowych nakazanie wyłączenia podstawowych serwerów sieci internetowej. Wskazanym rozwiązaniem jest przygotowanie sieci internetowej w Polsce do autonomicznego działania. Taka logiczna autonomia powinna być również zastosowana w odniesieniu do sieci internetowej na terenie UE. Należy przypuszczać, że taką logiczną autonomię sieci mają Rosja, Chiny, Indie oraz Izrael.

Szacuje się, że w 2025 roku w użyciu będzie 75 miliardów urządzeń Internetu Rzeczy. Współczesna infrastruktura przemysłowa jest złożona, obsługiwana przez różne podmioty, które, za sprawą urządzeń i aplikacji, są połączone wewnętrznie i zsieciowane z elementami zewnętrznymi. **Wrażliwych punktów może być wiele. Nie można dziś jednoznacznie wyznaczyć granicy między strefą bezpieczną i niebezpieczną. A cały system jest tak niezawodny jak poszczególne jego ogniwa.**

*Zespół Alertu Biznesowego dziękuje **Wacławowi Iszkowskiemu** za merytoryczną pomoc w przygotowaniu tego Alertu.*

Alert Biznesowy to inicjatywa think tanku Open Eyes Economy oraz Kolegium Gospodarki i Administracji Publicznej Uniwersytetu Ekonomicznego w Krakowie.

Wszystkie alerty eksperckie dostępne są na:
www.oees.pl/dobrzewiedziec