Nie bądź jak niemiecki muzealnik

opublikowano: wczoraj, 01-12-2019, 22:00

MAŁGORZATA GRZEGORCZYK @mag_pb email

Zarządzanie po polsku Muzeum w Dreźnie straciło miliard euro, bo stosowało przestarzałe zabezpieczenia. Cyfrowe złoto firm powinien chronić zarząd i pracownicy

W ostatni poniedziałek z Pałacu Królewskiego w Dreźnie skradziono zabytkową biżuterię wartą miliard euro. Przestępcy odłączyli prąd i nie zadziałał alarm, bo… nie miał zapasowego zasilania. Aż trudno uwierzyć, że w XXI w. udał się taki napad! Przecież żyjemy w czasach, gdy protestujący w Hongkongu świecą laserami w uliczne kamery, żeby oszukać stosowany przez chiński rząd system rozpoznawania twarzy. W październiku pojawiła się nawet wiadomość, że zakładają na głowy przenośne projektory, które wyświetlają na twarzach hologram przedstawiający innego człowieka. To akurat nieprawda — przenośne projektory to projekt artystyczny holenderskich studentów, ale technologia jest tak zaawansowana, że wiele osób dało się nabrać na tę plotkę (w tym jeden z występujących w poniższym tekście ekspertów).

PO LINII NAJMNIEJSZEGO OPORU: Pracownicy często bagatelizują kwestię bezpieczeństwa danych, działając dla własnej wygody, np....
Fot. Marek Wiśniewski

Złoto XXI wieku

Dzisiejszym odpowiednikiem złota są dane. A w Polsce to złoto jest słabo chronione.

— Rośnie świadomość RODO, ale na razie zasady dotyczące cyberbezpieczeństwa wprowadzają głównie firmy zagraniczne.Brytyjskie żądają od dostawców stosowania standardów ISO 21 regulujących bezpieczeństwo. Najbardziej świadome są branże e-commerce, bankowość, IT, a także automotive i przemysłowa, które wiedzą, że fabryki muszą być odizolowane i mieć własną infrastrukturę. Niestety, często firmy uświadamiają sobie zagrożenie dopiero w momencie, gdy jest już za późno — mówi Rafał Trzaska, dyrektor operacyjny firmy inżynieryjnej Bergman Engineering.

Tymczasem ataków będzie coraz więcej.

— Na razie stoją za nimi uzdolnieni hakerzy, ale gdy nauczą się tego zwykli Kowalscy, staną się powszechne. Już dziś można kupić kabel, który wygląda jak ładowarka, ale w środku ma mikroczip i po podłączeniu przejmuje kontrolę nad komputerem lub telefonem — dodaje Rafał Trzaska.

Zewsząd zagrożenie

W oszustwach pomaga technologia, np. narzędzia pozwalające naśladować głos innych osób. Zagrożeniem może stać się nieodpowiednio wprowadzone rozwiązanie chmurowe.

— Organizacje traktują priorytetowo transformację cyfrową, ale tylko 14 proc. budżetów cybernetycznych przeznacza się na zabezpieczenie wysiłków na rzecz transformacji. Reszta idzie na zakup usług i oprogramowania. W badaniu KPMG przeprowadzonym w ubiegłym roku wśród szwajcarskich firm 44 proc. przyznało, że nie ma narzędzi do kontrolowania jakości usług dostawców lub partnerów biznesowych, a 82 proc. nie ma planów na wypadek cyberataku. Czyli: firmy wysyłają dane do chmury obsługiwanej przez zewnętrznego partnera i mają nadzieję, że hakerzy nie zaatakują — mówi Paweł Wałuszko, menedżer ds. rozwoju biznesu, ekspert ds. cyberbezpieczeństwa w TestArmy.

Firmy nie zdają sobie sprawy, co im grozi. Z badania Deloitte wynika, że koszt wycieku danych szacują maksimum do 50 proc. rocznych przychodów. W rzeczywistości strata może być równa przychodom z 1-7 lat! Firma może być ukarana za wyciek danych, traci zaufanie klientów, a członkowie zarządu mogą zostać pociągnięci do odpowiedzialności karnej.

Najsłabsze ogniwo

Rodzajów cyberataków jest wiele, ale co do jednego eksperci są zgodni: najczęściej winny jest człowiek.

— Globalizacja i coraz częściej stosowany model pracy zdalnej wymusza na pracodawcach przydzielanie pracownikom zdalnego dostępu do danych firmowych. Stosowanie zaawansowanych zabezpieczeń, jak uwierzytelnianie wielopoziomowe, szyfrowanie urządzeń, połączenia VPN czy ograniczanie dostępów przy pracy z innej lokalizacji niż biuro, nie ogranicza jednak ryzyka związanego z wciąż najsłabszym ogniwem systemów informatycznych, jakim jest człowiek. Zaawansowane ataki socjotechniczne, w tym phishing, to najczęstsza przyczyna niepożądanych dostępów do systemów informatycznych — mówi Sylwia Pyśkiewicz, prezes Iron Mountain Polska.

Raport CERT potwierdził, że w 2018 r. stanowił on aż 44 proc. wszystkich odnotowanych incydentów. Według różnych szacunków w 50-80 proc. przypadków do ataków hakerskich dochodzi z powodu błędu pracownika lub obchodzenia zabezpieczeń sieci przez osoby pracujące.

Cała firma murem

Dlatego w ochronę spółki przed cyfrowymi zagrożeniami powinien być zaangażowany zarząd.

— Tak się nie dzieje: z badania 2019 Future of Cyber Survey przeprowadzonego przez Deloitte wśród amerykańskich firm z przychodami powyżej 500 mln USD wynika, że tylko 4 proc. osób

z poziomu zarządu: prezes, szef IT itd. omawia tematy związane z cyberbezpieczeństwem przynajmniej raz w miesiącu — mówi Paweł Wałuszko.

Problemem są też pracownicy niższego szczebla. 25 proc. specjalistów IT z ponad tysiąca amerykańskich firm powiedziało w tegorocznym badaniu Canona, że pracownicy nie tylko nie mają świadomości bezpieczeństwa, ale również nie rozumieją swojej roli w działaniach prewencyjnych.

— Firmy padają ofiarą oszustw polegających na podszyciu się pod osobę z kierownictwa, która rzekomo żąda zrobienia przelewu. Zdarzały się przypadki, gdy pracownicy angażowani przez przestępców do „tajnego projektu fuzji z inną firmą" organizowali tajne spotkania, żeby znaleźć sposób na wprowadzenie w błąd własnego działu księgowości i te przelewy wykonać — opowiada Cezary Piekarski, ekspert banku Standard Chartered zajmujący się cyberbezpieczeństwem (o sposobach oszustw firm więcej w ramce).

Jak się chronić

Eksperci podają receptę na cyberbezpieczeństwo.

— Bezpieczeństwo zaczyna się od obszarów organizacyjnych — wymagane jest stworzenie odpowiednich polityk i procedur (w tym BCP i DRP) oraz ustalenie cyklicznych szkoleń. Kluczowe jest zastosowanie odpowiednich technologii — zaawansowanych zapór sieciowych czy szyfrowania danych. Nie można zapominać również o obszarach ciągłego doskonalenia, przeglądach, aktualizacjach, audytach i testach — realizowanych również przez wyspecjalizowane podmioty zewnętrzne — wymienia Sylwia Pyśkiewicz.

— Firmy mogą się chronić dobrymi procedurami księgowymi, np. katalogiem kontrahentów, których numery kont są zapisane w umowie, a ich zmiana wymaga wielostopniowego zatwierdzenia. Warto współpracować z bankiem, bo banki oferują sposoby zarządzania rachunkami przedsiębiorców dostosowanymi do modelu płatniczego firmy, np. wielu drobnychodbiorców płatności lub kilku dużych, by nie wymagały złożonej autoryzacji — dodaje Cezary Piekarski.

Szybkie działanie

Co zrobić, jeśli mleko się już rozlało?

— Ważne, żeby przedsiębiorcy szybko reagowali i współpracowali z bankami oraz organami ścigania. System bankowy jest tak skonstruowany, że przy sprawnym działaniu można odzyskać część pieniędzy, bo przelewy między bankami nie zawsze odbywają się w czasie rzeczywistym. Jeśli przedsiębiorca najpierw dzwoni do prawnika, gdy ten jest niedostępny, czeka do kolejnego dnia, zgłoszenie na policję robione jest po trzech dniach, a wtedy pieniądze już dawno zostały wypłacone np. w Chinach i może być za późno na reakcję banku. Z bankiem i [illegible]

kontaktować się w pierwszej kolejności, jeśli tylko firma ma podejrzenie, że mogła paść ofiarą cyberprzestępstwa — mówi Cezary Piekarski.

Jak zaatakować firmę

NA DRUKARKĘ TestArmy dostała zlecenie sprawdzenia systemów i infrastruktury informatycznej firmy usługowej z oddziałami, która zatrudnia 2000 pracowników. Jej eksperci znaleźli lukę w zabezpieczeniu drukarki wi-fi. To umożliwiło dostanie się do infrastruktury firmy. Kolejnym krokiem było wejście w system monitoringu firmy, a dokładnie podpięcie się pod kamery — miedzy innymi sekretariatu. Dało to pełen podgląd dokumentów oraz pokoju prezesa, w tym jego biurka, ekranu laptopa i poczty.

NA REDAKTORA Atakujący podszywa się pod redaktora poczytnego serwisu internetowego. Dzwoni do firmy, prosząc o przeprowadzenie wywiadu, który później oczywiście będzie zautoryzowany. Rozmawia, zadaje pytania, a potem prosi o weryfikację firmy — kliknięcie w link do strony WWW wysłany na mejla. Osoba klika w link i tym sposobem pozwala na zaszycie złośliwego oprogramowania. Co za tym idzie? Bezpośredni lub pośredni atak na konkretną osobę lub na całą infrastrukturę.

NA PIZZĘ Pracownicy dostają mejle z informację o otwarciu w okolicy pizzerii (istnieje fałszywa strona WWW), która pierwszym klientom oferuje 30 proc. zniżki. Zrzucają się na zamówienie. Po kilkudziesięciu minutach pojawia się dostawca z zamówionym jedzeniem (na pudełkach logo fikcyjnej firmy) i gratisem — ledowymi lampkami na USB zmieniającymi kolor w rytm muzyki. W lampki wbudowane są pendrive'y ze złośliwym oprogramowaniem. Pracownicy podłączają je do komputerów. Kilka minut później firmowa sieć przestaje działać, bo haker uzyskuje zdalny dostęp do urządzeń i szyfruje wszystkie dane w firmowym systemie.

NA DOSTAWCĘ Cenzin z Polskiej Grupy Zbrojeniowej stracił kilka milionów złotych, które wpłacił cyberprzestępcom. Podszyli się pod dostawcę broni z Czech, który jakoby zmienił numer konta. Pracownicy Cenzinu nie zweryfikowali wysłanych mejlem informacji o nowym numerze, na który należało uiszczać płatności.

NA KLIENTA Dane o firmie haker uzyskuje ze internetu. Dowiaduje się o jej kontraktach i partnerach biznesowych. Następnie dzwoni do firmy i podszywa się pod klienta lub partnera („pracujecie dla mnie od pięciu lat!") i apodyktycznie żąda podania natychmiast poufnych danych. Część osób ulega presji.

Zarządzanie po polsku

Redakcja „Pulsu Biznesu" po raz trzeci zmierzy się z tematem dotyczącym stylu zarządzania przedsiębiorstwem przez polskie menedżerki i menedżerów. Tegoroczna edycja będzie składała się z dwóch części: badania ankietowego wśród menedżmentu oraz rozwinięcia na łamach „PB" najważniejszych wyzwań stojących przed polskimi spółkami. Poza opisywana[illegible]

pozyskiwania pracowników interesują nas m.in. zagadnienia: — polityka różnorodności w przedsiębiorstwie — skuteczna analityka danych oraz wdrożenie zmian wynikających z big data — bezpieczeństwo cyfrowe. Partnerem merytorycznym tegorocznej edycji „Zarządzania po polsku" jest EY, międzynarodowa firma świadcząca usługi doradcze i audytorskie. Zapraszamy do śledzenia projektu na łamach „Pulsu Biznesu" i na pb.pl/popolsku.

Podpis: Małgorzata Grzegorczyk

Z ostatniej chwili

17:15 Produkcja OPEC znów spadła

16:35 Zużycie paliw płynnych wzrosło po trzech kwartałach o 4 proc.

16:01 USA: wydatki na inwestycje budowlane nieoczekiwanie zmniejszyły się

16:00 USA: spadł indeks ISM dla przemysłu

15:45 USA: indeks PMI dla przemysłu lepszy od oczekiwań

WIĘCEJ