Bezpieczeństwo organizacji w kontekście pandemii COVID-19

Pierwsze półrocze 2020 roku zmieniło nasze życie zawodowe, prywatne oraz społeczne. Gdy w Polsce świętowaliśmy Nowy Rok, w Chinach narastało nowe zagrożenie, które w krótkim czasie dotarło i do nas. Niewielu umiało to przewidzieć, większość odrzucała myśl, że wydarzenia gdzieś w dalekich krajach będą miały tak dojmujący wpływ na biznes i gospodarkę światową. Dużo firm stanęło przed pytaniem – co dalej?

Piotr Słupczyński
Członek Krajowego Stowarzyszenia Ochrony Informacji Niejawnych

Co się kryje pod hasłem „cyberbezpieczeństwo"?

Nikt nie wiedział, jak długo ta sytuacja się utrzyma i ile potrwa przymusowe przeniesienie naszego życia do cyberprzestrzeni. Czy firmy i pracownicy byli na to przygotowani? Co z prawnie chronionymi tajemnicami? Czy poufne informacje przedsiębiorstwa nadal będą bezpieczne? W Polsce jest ponad sześćdziesiąt rodzajów tajemnic prawie chronionych, więc obaw było wiele.

W niektórych organizacjach praca zdalna była codzienną praktyką, jednak dla większości to nowy temat. Firmy w krótkim czasie musiały przejść na pracę online, często bez wcześniejszych testów. To nowe i trudne wyzwanie dla organizacji. Zachowanie cyberbezpieczeństwa stało się priorytetem.

Co się składa na cyberbezpieczeństwo?

• Software i hardware, czyli antywirusy i firewalle oraz wiele innych rozwiązań tego typu.
• Dostęp do sieci, czyli bezpieczne i stabilne połączenie z firmą. Jeśli do sieci w danym gospodarstwie domowym podłączonych jest kilka komputerów korzystających z oprogramowania do komunikacji, przepustowość zwykłego łącza może nie wystarczyć.
• Edukacja – szkolić, szkolić i jeszcze raz szkolić! Można korzystać z antywirusa i innych zabezpieczeń, jednak to właśnie człowiek jest najsłabszym ogniwem. Jest podatny na określone działania. Jeśli wyślę Państwu wiadomość z informacją, że została wynaleziona szczepionka na COVID-19 i będzie ona testowana, zapewne część odbiorców kliknie w załączony link, który może zawierać złośliwe oprogramowanie.
• „Polityka bezpieczeństwa", „Zasady bezpieczeństwa", „Regulamin pracy zdalnej" czy „Dobre praktyki". Dokumentacja to bardzo ważny element bezpieczeństwa. Dobrze napisane dokumenty zawierające analizę ryzyka zapewniają określenie właściwego poziomu zagrożenia wraz z dobraniem odpowiednich środków bezpieczeństwa. Eliminuje to złe nawyki użytkowników. W dokumentacji można dookreślić m.in. kwestie incydentu lub postępowanie w przypadku utraty dostępu do dedykowanego kanału komunikacji w firmie.
• Regularne audyty – dzięki nim firma dostaje informację zwrotną o lukach w zabezpieczeniach. Audyt to świadoma decyzja zarządu, czasem bolesna, lecz zawsze kończy się zaleceniami, które warto wdrożyć.
• Regulacje prawne – ustawy i akty wykonawcze np. ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych, Tarcza 4.0 i wiele innych, zależnych od profilu działalności przedsiębiorstwa.

Jakie są potencjalne zagrożenia w cyberprzestrzeni?

Podobnie jak Covid-19, zagrożenie w świecie cyfrowym może sparaliżować funkcjonowanie organizacji. Kto stoi za atakami? Haker, wbrew przekonaniom, nie nosi za dużych swetrów, nie siedzi w kapturze w ciemnym pomieszczeniu, odseparowany od ludzi. Obecnie są to profesjonalnie zorganizowane grupy przestępcze, inwestujące duże pieniądze w rozwój i sprzęt. Atak na firmę jest długim i przemyślanym procesem. Prawie zawsze chodzi o pieniądze, lecz zdarzają się też ataki aktywistów lub pojedynczych samotnych wilków. Grupy hakerskie często wspierane są przez rządy państw totalitarnych i nie tylko. W ubiegłym miesiącu w Darknecie można było za 200 dolarów wykupić atak hakerski na wybraną firmę z możliwością wideorelacji.

Jak oszust przejmuje kontrolę nad komputerem i uzyskuje dostęp do zasobów sieciowych, wykorzystując ludzką podatność? Cyberprzestępca przy pomocy np. pamięci USB, załącznika lub linku przesłanego mailem infekuje komputer ofiary, instalując złośliwe oprogramowanie. Następnie haker robi rekonesans. Sprawdza, co ciekawego znajduje się na komputerze i do jakich zasobów zdobył dostęp. Może zainstalować programy monitorujące kolejność naciskania klawiszy na klawiaturze, dzięki czemu wykrada loginy i hasła dostępowe. Jest w stanie przejąć kontrole nie tylko nad komputerem, telefonem czy siecią, lecz także nad usługami chmury, mediów społecznościowych, banków lub prywatnej poczty. Nie łudźmy się, że komputer będzie błyskał czerwonym światłem, gdy zostanie zaatakowany. W interesie cyberprzestępcy jest pozostać jak najdłużej w ukryciu. Haker uczy się naszych przyzwyczajeń i zachowań. Na koniec ataku może usunąć wszystkie kopie zapasowe, do których ma dostęp, zaszyfrować dysk i zażądać okupu za odszyfrowanie. Ostatnio spotkałem się z tym, że hakerzy żądają zapłaty za nieujawnienie danych.

Możliwe warianty cyberataków

Przedstawię Państwu dwa scenariusze ataku z wykorzystaniem socjotechniki, czyli jak w informatyce wygląda „kradzież na wnuczka".

W upalne lato pewna filia znanej międzynarodowej korporacji została zaatakowana w sprytny sposób. Na służbowe adresy poczty internetowej przed porą lunchu trafiła informacja o nowo otwartej pizzerii. W wiadomości była oczywiście strona internetowa lokalu wraz z menu oraz informacja o niespodziance dołączonej do każdego zamówienia. Pracownicy szybko zdecydowali się na zamówienie, po pięćdziesięciu minutach zjawił się dostawca. Po przyjęciu zapłaty przekazał pizzę i niespodziankę w postaci wiatraczków zasilanych przez wejście USB. Niczego nieświadomi pracownicy podłączyli urządzenia do kom-

puterów. Poza możliwością przyjemnego ochładzania urządzenia posiadały złośliwe oprogramowanie, dzięki któremu można było przejąć kontrolę nad firmowymi komputerami. Całe szczęście był to kontrolowany audyt zamówiony przez firmę. Strach pomyśleć, ile urządzeń ze złośliwym oprogramowaniem jest podłączanych przez nieświadomych użytkowników i jakie szkody może to przynieść organizacji. Czy ktoś w Państwa firmach to kontroluje?

Kolejnym przykładem sprytnego ataku jest atrakcyjny anons na jednym z portali ogłoszeniowych. Haker zamieścił informację: „Mieszkanie 2-pokojowe 45m2 do wynajęcia, 2300 PLN Centrum" z atrakcyjnym opisem, pięknym zdjęciem, adresem e-mail, numerem telefonu i prośbą, by kontaktować się przez SMS motywowaną brakiem możliwości rozmowy w pracy. Interesant wysyła SMS-a z zapytaniem: „czy ogłoszenie aktualne?". Następuje wymiana wiadomości. Haker z uwagi na wygodę zaleca komunikację e-mail. Ofiara zwraca się z prośbą o dodatkowe zdjęcia mieszkania. Oszust proponuje, że prześle plik 360° z rozkładem mieszkania. Ofiara zgadza się, a cyberprzestępca wysyła wiadomość z prezentacją lokalu. Jednak poza obiecanym wirtualnym spacerem w pliku jest zaszyte złośliwe oprogramowanie. Daje to hakerowi dostęp do komputera i danych.

Jak się bronić przed socjotechnikami?

Należy zachować szczególną ostrożność, wyłączyć emocje i włączyć racjonalne myślenie. Wiadomości e-mail lub SMS z wyjątkowymi okazjami, dziwnymi plikami, linkami do płatności lub przelewów należy usuwać albo zgłaszać do wewnętrznych działów IT. Jeśli IT działa prawidłowo, zgłosi to do CERT POLSKA (incydenty.cert.gov.pl). Tylko działanie zespołowe podnosi zbiorową odporność oraz świadomość pracowników.

Państwo kontra hakerzy

Hakerzy są bardzo pomysłowi, doskonale przystosowują się zmieniającego się prawa, co chwila wymyślając nowe scenariusze ataku. Od 1 stycznia br. obowiązuje Indywidualny Rachunek Podatkowy. Już 22 stycznia Ministerstwo Finansów ostrzegało o rozsyłanych przez oszustów wiadomościach dotyczących zaległości na mikrorachunku podatkowym z prośbą o dopłatę w kwocie 6,18 zł. Podobnie ma się sprawa z bonem turystycznym. Kolejnym scenariuszem jest użycie zainfekowanego komputera i jego adresu IP do ataku na jakąś instytucję państwową lub infrastrukturę krytyczną, ale to zostawiam Państwa wyobraźni.

W połowie czerwca 2020 roku Premier Australii Scott Morisson oświadczył na konferencji prasowej, że od dłuższego czasu jego kraj jest obiektem ataków hakerskich. Poza obywatelami oraz urzędami, ofiarą padła infrastruktura krytyczna; operatorzy telekomunikacyjni, przemysł, służba zdrowia i wiele innych podmiotów. Wspomnę, że Australia domagała się międzynarodowego śledztwa w sprawie COVID-19. Niewątpliwie mamy tu do czynienia z wojną w cyberprzestrzeni.

Dobrym podsumowaniem ataków w 2019 roku jest Raport roczny z działalności CERT Polska „Krajobraz bezpieczeństwa polskiego Internetu w 2019 roku" dostępny na www.cert.gov.pl. Z dokumentu wynika, że zgłoszeń w stosunku do roku poprzedniego przybyło o 71 proc. W 2020 roku zgłoszeń i ataków będzie na pewno o wiele więcej.

Co firma może stracić, jeśli nie zadba o bezpieczeństwo?

Przede wszystkim ryzykuje wyciek danych osobowych. RODO przewiduje karę dla prywatnych firm do 20 000 000 EUR lub 4 proc. światowego obrotu. Ponadto organizacja może utracić swoje know-how – projekty, pomysły czy tajemnice przedsiębiorstwa. Jeśli hakerzy będą sprytni i cierpliwi, mogą zaplanować czasowe sekwencyjne wyłączenie serwerów i komputerów bądź zaszyfrowanie danych. W praktyce uniemożliwi to działanie firmie, powodując mały informatyczny blackout. Do tego dochodzą liczne pozwy cywilne oraz odpowiedzialność karna. Są jeszcze inne wartości, których nie można wycenić, np. wizerunek firmy, który buduje się latami.

Znaczącą rolę w bezpieczeństwie organizacji odgrywa świadomość użytkowników. Dobrze wyedukowany i racjonalnie zachowujący się pracownik jest dla firmy niesamowitą wartością. Dzięki jego doświadczeniu i wiedzy, przy odpowiednich procedurach, politykach bezpieczeństwa oraz wsparciu działu IT, można odpowiednio wcześniej reagować na próby ataku.

Jak bronić się przed atakiem?

Najtańszą metodą jest edukacja. Trzeba stale podnosić świadomość informatyczną zarówno kadry zarządzającej, jak i szeregowych pracowników. Proces uświadamiania musi być ciągły i regularny przez uczestnictwo w szkoleniach, warsztatach, konferencjach lub kongresach. Organizator powinien mieć co najmniej kilkuletnie doświadczenie i przynależeć do Rejestru Instytucji Szkoleniowych. Nauczanie podnosi świadomość, a ta otwiera oczy. Dzięki temu można stworzyć i wdrożyć odpowiednie procedury. Mają one sens, gdy są procesem, na który składa się ciągła edukacja i doświadczenie. Nie sztuką jest spisanie polityk i procedur językiem informatycznym oraz trzymanie ich w sejfie. Mistrzostwem jest stworzenie dokumentów zrozumiałych dla każdego i łatwo dostępnych, a jednocześnie ujawniających jak najmniej informacji, które mógłby wykorzystać haker. Wiedza i doświadczenie pracowników to majątek organizacji.

Konferencje i wydarzenia o tematyce cyberbezpieczeństwa

W dniach 19–20 października br. odbędzie się 10. Konferencja Bezpieczeństwa Narodowego i Gospodarczego uwzględniająca zagrożenia COVID-19 (konferencjabezpieczenstwanarodowego.swbn.pl). W ubiegłym roku uczestników zaszczycił swoją obecnością i wykładem Pan Prezydent Aleksander Kwaśniewski. W tym roku zapraszamy również przedstawicieli służby zdrowia, a gościem specjalnym będzie prof. Krzysztof Simon.

Kolejnym wydarzeniem o tematyce bezpieczeństwa i ochrony tajemnic firmy jest III Krajowy Zjazd Pracowników Pionów Ochrony Informacji Niejawnych, który odbędzie się w dniach 7–9 grudnia 2020 roku w Białce Tatrzańskiej. Spotkanie organizowane jest nieprzerwanie od piętnastu lat pod nazwą Forum Kierowników Jednostek Organizacyjnych oraz Pełnomocników Ochrony Informacji Niejawnych. Uczestniczyłem w dwóch poprzednich zjazdach. Można spotkać tam osoby z różnych jednostek organizacyjnych. Posiadam kilkunastoletnie doświadczenie w pionie ochrony i uważam, że każdy pracownik zajmujący się zarządzeniem bezpieczeństwem, ochroną danych osobowych czy tajemnicą przedsiębiorstwa powinien wpisać ten termin do kalendarza. Wiedza, którą przekazują prelegenci, łączy w sobie praktykę oraz informacje mające zastosowanie nie tylko dla pionu ochrony informacji niejawnych, lecz także dla działów bezpieczeństwa, IT, HR, ISO, infrastruktury krytycznej, prezesów, zarządów czy kadry kierowniczej.

Za wartość dodaną obu tych wydarzeń uważam możliwość wymiany doświadczeń i rozmów kuluarowych pomiędzy uczestnikami oraz prelegentami. Przemyślane i dobrze zaplanowane krótkie, 20-minutowe wystąpienia zapewniają ciągłe skupienie słuchaczy. Organizatorzy zadbali o prawidłową równowagę umysłu, dając uczestnikom czas wolny oraz tematyczne atrakcje.

Zapewne tegoroczna konferencja oraz zjazd będą wyjątkowe i równie emocjonujące co poprzednie. Wpływ pandemii COVID-19 na gospodarkę oraz szeroko pojęte bezpieczeństwo będzie ważnym tematem przewodnim. Będę prelegentem podczas tych wydarzeń, więc zapraszam do rejestracji na stronie www.ksoin.pl ■