Ireneusz Piecuch,
Starszy Partner, DGTL Kibil Piecuch i Partnerzy S.K.A.

Cyberbezpieczeństwo w czasach kryzysu

Raport Cost of A Data Breach 2020 opublikowany właśnie przez IBM, nie pozostawia złudzeń. Prawie 80% badanych przedsiębiorstw jest przekonana, że pandemia wpłynie na pogorszenie możliwości sprawnego reagowania na ataki. Wśród ponad 500 badanych przedsiębiorstw z kilkunastu krajów na świecie, które padły ofiarą hackerów, średnie szkody wyrządzone tymi atakami wynoszą prawie 3.9 mln dolarów. Aczkolwiek raport publikowany jest za okres tylko częściowo obejmujący czas pandemii, to jego autorzy obliczają, że sama praca zdalna spowodowała wzrost wysokości średniej szkody o 137 tysięcy dolarów. Co jeszcze bardziej niepokojące, średni czas niezbędny do odkrycia podatności i podjęcia skutecznych działań to 280 dni - ponad 9 miesięcy!

Sytuacja wywołana wystąpieniem wirusa Covid-19 zmusiła wiele przedsiębiorstw do przejścia na zarządzanie kryzysowe i niejednokrotnie przestawienia się na pracę zdalną. Praca zdalna nie jest oczywiście niczym nowym, jednakże skala niezbędnych do podjęcia działań zaskoczyła wiele z nich. Pierwszym problemem okazała się dostępność sprzętu nadającego się do pracy. Okazało się też, że procesy i procedury obowiązujące w niektórych firmach, nie były właściwie przystosowane do nowych warunków. Zarządzanie zespołami w nowych warunkach stanowi kolejną przeszkodę. Jednak elementem, który jest jednym z większych wyzwań nowej rzeczywistości jest cyberbezpieczeństwo. Niski poziom świadomości zagrożeń z tym związanych sprzed czasów epidemii, wykazywany w wielu badaniach, w połączeniu ze wzrostem ataków typu phishing i ransomware, sprawił, że wiele przedsiębiorstw stało się podatnych na ataki jak nigdy dotąd. Korzystanie z domowych routerów wi-fi, bardzo często z niezmienionymi fabrycznymi ustawieniami, wykonywanie na jednym komputerze zadań służbowych i prywatnych, wysoka podatność na działania socjotechniczne spowodowane obawami przez narastającą falą zakażeń - to tylko niektóre elementy sprzyjające tym wszystkim, którzy postanowili zwiększyć częstotliwość ataków hackerskich wyczuwając w pandemii nadarzającą się okazję.

Wyniki raportu IBM pokazują, że złośliwe oprogramowanie odpowiada za 52% wszystkich badanych przypadków. Z tych 52% aż 14% można przypisać atakom typu phishing, a 19% przypadkom przejęcia danych upoważniających do dostępu do danych. Szczególnie ta pierwsza kategoria okazała się bardzo użyteczna w czasach, w których stres powodowany obawą przed zakażeniem, dużym chaosem informacyjnym w pierwszych miesiącach pandemii i wydaje się, że pełne skutki tych ataków poznamy dopiero za kilka, czy może nawet kilkanaście miesięcy.

Cyberbezpieczeństwo nie należało na ogół do priorytetów działań podejmowanych przez firmy dotknięte ograniczeniami związanymi z pandemią. Dla większości zarządzających, zmiany wywołane przez Covid-19, stanowiły przede wszystkim zagrożenie dla stabilności finansowej firm - ryzyko gwałtownej utraty przychodów przy jednoczesnej konieczności utrzymywania

niezmienionego poziomu kosztów. Nic więc dziwnego, że większość działań podejmowanych w trybie zarządzania kryzysowego dotyczyła tych dwóch właśnie elementów. Tam, gdzie wydatki były absolutnie niezbędne (przykładowo zakup nowych komputerów), podejmowano je z ciężkim sercem. Tam jednak, gdzie ryzyko wydawało się być odległe i kiepsko zdefiniowane (a tak w dużej mierze postrzegane są w dalszym ciągu cyberzagrożenia), podjęcie decyzji odkładano na później.

Warto zaznaczyć, że zdaniem autorów raportu IBM, ponad 40% szkód wynikających z ataków hackerskich to właśnie związane z nimi utracone przychody przedsiębiorstwa. Czy zatem w czasach gwałtownie zachodzących zmian, a w takim świecie przychodzi nam właśnie funkcjonować, właściwie ustawiamy priorytety naszych przedsiębiorstw?

Wydaje się, że wielu zarządzających nie do końca docenia stopień uzależnienia swoich firm od poprawnego działania systemów informatycznych. To dość poważny problem, bo w obecnych czasach nawet przedsiębiorstwa, które trudno zakwalifikować jako działające w obszarze gospodarki cyfrowej, w coraz większym stopniu uzależniają swoją ciągłość działania od technologii cyfrowych. Wystarczy spojrzeć na zestawienie wysokości strat poniesionych na skutek cyberataków według branż. Otóż branża technologiczna zajmuje dopiero piąte miejsce, podczas gdy na czele znajduje się sektor zdrowia, sektor energetyczny, sektor finansowy i sektor farmaceutyczny.

Należy pamiętać, że atak typu ransomaware jest w stanie pozbawić firmę przestawioną na pracę zdalną możliwości działania. Przy ograniczeniach dotyczących możliwości wykorzystania przestrzeni biurowych (połączonych ze zwiększonym ryzykiem infekcji) może się okazać, że jedynym możliwym wyjściem będzie zapłata okupu. Ostatnio jeden z portali zajmujących się cyberbezpieczeństwem opublikował zapis negocjacji z hackerami w tym zakresie. Skończyło się na 4.5 mln dolarów i wymianie grzeczności. A co jeśli przedsiębiorstwo nie dysponuje takimi środkami? Okup nie jest zresztą najgorszym co może się zdarzyć. Firmy takie jak Mersk czy Aramko odmówiły zapłaty i wydały setki mln dolarów na ponowne przywrócenie operacji w swoich firmach, choć ich ustabilizowanie zajęło miesiące. To jednak nie wszystko. Equifax po ataku hackerskim, nie tylko wydał setki mln dolarów na infrastrukturę techniczną, ale musiał także zapłacić kwotę dochodzącą niemalże jednego mld dolarów należną w formie kar i ugód urzędom regulacyjnym oraz osobom pokrzywdzonym. Jak zatem widać pytanie czy przetrwanie, w przypadku cyberzagrożeń nie musi być postrzegane jako dylemat. W istocie bowiem, większość skutecznych ataków hackerskich w pierwszej mierze odbije się na wynikach finansowych firmy, a niektóre z nich mogą doprowadzić do jej upadku. Nakłady na cyberbezpieczeństwo, są zatem nie tyle kosztem, co inwestycją w zabezpieczenie przychodów i przetrwania firmy.

Co więcej, zmiana stopnia podatności firmy na cyberataki, nie zawsze sprowadza się do inwestycji w infrastrukturę informatyczną. Zgodnie z badaniami, olbrzymia część skutecznych ataków hackerskich związana jest z wystąpieniem błędu ludzkiego. Czasami, są to błędy związane z utrzymaniem infrastruktury (przykładowo tolerowanie znanej już podatności systemu, której można byłoby zapobiec i odsuwanie w czasie jej usunięcia - Equifax). Dużo częściej jednak jest to brak elementarnej wiedzy o istocie ryzyka oraz nieznajomość sposobów radzenia sobie w sytuacji, w której ryzyko takie się realizuje. Wszyscy znamy ćwiczenia przeciwpożarowe mające na celu weryfikację przygotowania osób pracujących w danym budynku do jego opuszczenia. A jak często przedsiębiorstwa organizują takie ćwiczenia, pozorując atak hackerski? Jak często zatrudniają firmy mające regularnie atakować infrastrukturę IT, aby tym sposobem pozyskać wiedzę o słabościach tych systemów?

Autorzy raportu IBM jednoznacznie wskazują, że utworzenie specjalnych struktur zajmujących się reagowaniem na incydenty, czy regularnie przeprowadzane testy skuteczności systemu zarządzania bezpieczeństwem informacji przyczyniają się do tego, że poziom strat pomiędzy przedsiębiorstwem, które wdrożyło takie działania, a przedsiębiorstwem, które nie zdecydowało się na ich wprowadzenie wynosi średnio 2 mln dolarów.

Nawet pobieżna lektura raportu IBM pokazuje, że cyberbezpieczeństwo jest jednym z elementów krytycznych pozwalających na zachowanie ciągłości działania przedsiębiorstwa, jego zdolności do generowania przychodów, a niejednokrotnie także utrzymanie poziomu jego konkurencyjności na rynku (np. na rynku finansowym). Raport ten (a w zasadzie jeden jego mały fragment), pokazuje jednak także dlaczego w wielu przypadkach cyberbezpieczeństwo ma problem z przebiciem się do puli głównych priorytetów działalności firmy. Otóż, zgodnie z tym raportem w 30% przypadków, zaatakowane firmy nie były w stanie wskazać jednej konkretnej funkcji, do której przypisana byłaby kwestia odpowiedzialności za wystąpienie incydentów. Aż w 46% przypadków odpowiedzialność taką przypisywano CISO, w 25% na CIO/CTO, a jedynie w 12% na CEO/COO (w badaniu dopuszczano możliwość wskazania kilku funkcji). Problem polega na tym, że to nie CISO decyduje w firmie o wielkości nakładów, środków i zasobów na cyberbezpieczeństwo. Wydaje się, że dopóki ten stan nie ulegnie zmianie, cyberbezpieczeństwo może dla wielu przedsiębiorstw, okazać się prawdziwą piętą achillesową, szczególnie w czasach zawirowań i turbulencji na rynku.

□