SKwP

Cyberprzestępcy są zagrożeniem dla księgowych

Złośliwe oprogramowanie może zniknąć i zatrzeć ślady swojej aktywności. Jak księgowy udowodni, że wpisując inny numer konta, albo nie podmienił go celowo, współdziałając z przestępcami?

Firmy wiedzą za mało

DANE | Złośliwe oprogramowanie może zniknąć i zatrzeć ślady swojej aktywności. Jak księgowy udowodni, że w ogóle doszło do ataku i nie popełnił błędu, wpisując inny numer konta, albo nie podmienił go celowo, współdziałając z przestępcami?

TOMASZ GAŁECKI

PIOTR HANS

Stowarzyszenie Księgowych w Polsce

Cyberzagrożenia to modny temat. Coraz bardziej nasila się przekonanie, że nikt nie jest bezpieczny, nawet największe i najbardziej znane światowe firmy technologiczne, a co dopiero mali czy średni polscy przedsiębiorcy. Bezpieczeństwo informatyczne znalazło się w obszarze zainteresowania nie tylko informatyków, ale także członków zarządów i rad nadzorczych. Czy ma ono znaczenie także dla pracy i bezpieczeństwa księgowych?

Skala problemu

„Cyberprzestrzeń stała się naszym naturalnym środowiskiem i siłą rzeczy zagrożenia z «prawdziwego» świata przeniosły się również do internetu. (...) Wykrywanie incydentów i usuwanie ich skutków to jedno, ale wyedukowany użytkownik równie skutecznie sam może zapobiegać zagrożeniom. Czasy, gdy to nam instalowano wirusa minęły, teraz robimy to nieświadomie sami. Dziś cyberprzestępca nie musi się znać na złośliwym oprogramowaniu – zwyczajnie może je kupić".

Przytoczone cytaty pochodzą z raportu „Raport CERT Orange Polska za rok 2016", z którego wynika jednoznacznie, że skala zagrożeń w cyberprzestrzeni jest już znacząca i nadal będzie rosła. Obecnie odnotowuje się ponad 17 tys. incydentów bezpieczeństwa w ciągu roku. Co piąty z nich to próba włamania, co piętnasty – przypadek złośliwego oprogramowania. A to tylko częściowy obraz zagrożeń w polskim internecie.

Inny raport, „Badanie rynku cyberbezpieczeństwa w Polsce 2017", przeprowadzony na zlecenie T Mobile w niemal 700 dużych i średnich firmach, mówi o tym, że 51 proc. średnich przedsiębiorstw i 45 proc. dużych spółek zadeklarowało, że nie padło do tej pory ofiarą cyberataku. Czy to świadczy o naszym bezpieczeństwie? Niestety nie, raczej o niskiej świadomości zagrożeń. Jak wskazują autorzy raportu, brakuje w polskich firmach monitoringu i rejestracji tego typu zdarzeń.

Dowodzi tego również piąta edycja raportu „Zarządzanie ryzykiem i ubezpieczeniami w firmach w Polsce 2017/2018" Aon Polska, podmiotu zajmującego się zarządzaniem ryzykiem, pośrednictwem ubezpieczeniowym i reasekuracyjnym. Raport pokazuje bowiem, że wbrew ogólnoświatowej tendencji przestępczość komputerowa nie jest uważana przez polskich przedsiębiorców za ryzyko kluczowe (na liście najważniejszych ryzyk zajmuje dopiero 19 miejsce, podczas gdy w ogólnoświatowych wynikach zajmuje piątą pozycję, a w Ameryce Północnej – stanowi obecnie największe zagrożenie).

Jakie czynniki sprawiają, że skala zagrożeń cybernetycznych cały czas rośnie? Autorzy raportu „MMC Cyber Risk Handbook 2018" – specjaliści z firmy Marsh & McLennan Companies, zajmującej się ubezpieczeniami i zarządzaniem ryzykiem – wskazują na dwie główne tendencje:

- z jednej strony, branża cyberprzestępczości jest już dojrzała i działa na wielką skalę (Europol szacuje, że już w tej chwili globalne straty wynikające z działalności cyberprzestępców wynoszą rocznie ponad 290 mld euro, czyli więcej niż zyski karteli narkotykowych),
- z drugiej strony, coraz bardziej otaczająca nas technologia zaciera granice pomiędzy światem cyfrowym i fizycznym (od smartfonów poczynając, poprzez autonomiczne auta, na inteligentnych termostatach czy żarówkach kończąc).

Niebezpieczeństwo dla firm...

„Wiele wskazuje na to, że rok 2017 okaże się rokiem *phishingu*, przygotowywanego pod konkretne grupy zawodowe, co może znacznie wpłynąć na jego skuteczność. Księgowy z większym prawdopodobieństwem otworzy odpowiednio nazwany plik excela, a jeśli przestępca, usiłujący zaatakować naszą firmę znajdzie wcześniej na Facebooku czy Linkedin odpowiednich kandydatów, szanse jego powodzenia wyraźnie wzrosną."

To kolejny cytat ze wspomnianego raportu CERT Orange Polska. Jego autorzy diagnozują, że grupą zawodową, znajdującą się w obszarze szczególnego zainteresowania cyberprzestępców, mogą być księgowi – strażnicy firmowych pieniędzy.

Dlaczego tak się dzieje? Działa tu zimna kalkulacja, oparta na przewidywanej większej efektywności działania, wywołanej przez iloczyn dwóch czynników: prawdopodobieństwa i skutku. Przeciętny Nowak wykonuje w ciągu miesiąca raczej ograniczoną liczbę