KPMG

COVID-19 jak ustrzec się przed cyberatakiem ?

Pandemia COVID-19 zmienia nasze dotychczasowe życie. Wzrost zaniepokojenia społeczeństwa zaistniałą sytuacją idzie w parze ze wzrostem zapotrzebowania na informacje, oraz zapewnienie bezpieczeństwa i wsparcia. Zorganizowane grupy cyberprzestępcze skutecznie wykorzystują niepewność i obawy związane z pojawieniem się koronawirusa do atakowania osób prywatnych i przedsiębiorstw na przeróżne sposoby.

Zagrożenia

Od połowy lutego KPMG zaobserwowało błyskawiczny rozrost infrastruktury wykorzystywanej przez cyberprzestępców do prowadzenia ukierunkowanych kampanii phisingowych (ang. spear-phishing) związanych tematycznie z COVID-19. Kampanie te miały na celu zwabienie nieświadomych użytkowników na fałszywe strony internetowe i wyłudzenie ich danych uwierzytelniających do usługi Office365.

Przykłady zrealizowanych kampanii obejmują:

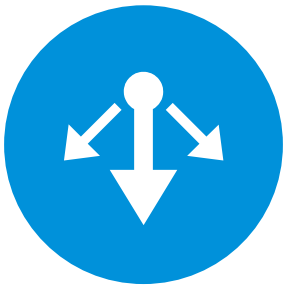
- Wiadomości mailowe dotyczące tematu COVID-19 z załącznikami wykorzystującymi znaną podatność systemów Microsoft do uruchomienia złośliwego kodu
- E-maile phishingowe, których załączniki - dokumenty programu Microsoft Word z informacjami o tematyce zdrowotnej - zawierały makra służące pobraniu złośliwego oprogramowania Emotet lub Trickbot
- Wiadomości zachęcające do odwiedzenia fałszywych kopii strony CDC (Centre for Disease Control) wymagających od użytkowników podania danych uwierzytelniających
- Szereg fałszywych usług doradczych rzekomo mających na bieżąco informować klientów o przerwach w świadczeniu różnych usług z powodu pandemii, w rzeczywistości służących do rozpowszechniania złośliwego oprogramowania
- Fałszywe maile podszywające się pod Ministerstwo Zdrowia bądź Światową Organizację Zdrowia (WHO) z zaleceniami odnośnie środków ostrożności w czasie pandemii COVID-19, w rzeczywistości zawierające również złośliwe oprogramowanie
- Fałszywe oferty ulg podatkowych związanych z pandemią, kierujące adresatów na strony wyłudzające ich dane podatkowe i finansowe.

Wiele istniejących zorganizowanych grup przestępczych zmieniło swoje taktyki działania, coraz częściej wykorzystując w przeprowadzanych atakach materiały związane z koronawirusem takie jak wiadomości medyczne, informacje o fałszywych lekarstwach, dodatkowych świadczeniach w sytuacjach kryzysowych i brakach w zaopatrzeniu.

Typowe sygnały, mogące świadczyć, że e-mail jest elementem ataku phishingowego to:

- Błędy gramatyczne, interpunkcyjne i literówki w treści wiadomości
- Forma i jakość wiadomości pozostawiająca wiele do życzenia
- Wiadomość nie adresowana bezpośrednio do konkretnego odbiorcy, lecz rozpoczynająca się od ogólnych zwrotów: Szanowny Panie/Pani, Drogi kliencie itp.
- E-mail zawierający bezpośrednią prośbę o podanie danych uwierzytelniających osobowych lub bankowych.
- Oczywiście należy też pamiętać, jeśli treść wiadomości brzmi zbyt pięknie, by mogła być prawdziwa, to prawdopodobnie tak jest.

Materiał jest tłumaczeniem broszury KPMG pt.: „COVID-19 Staying cyber secure" opublikowanej 19 marca 2020. Skład i modyfikacje treści w języku polskim KPMG w Polsce.



Istnieją sposoby, które pomogą ograniczyć ryzyko, z którym mierzy się Państwa organizacja i jej pracownicy, szczególnie w przypadku przejścia na model zdalnej pracy. Są to między innymi:

Reakcja

- Podnoszenie świadomości pracowników na temat zwiększonego ryzyka ataków phishingowych związanych tematycznie z COVID-19.
- Udostępnianie wiarygodnych materiałów informacyjnych na temat zasad bezpieczeństwa oraz regularna komunikacja z pracownikami na temat podejścia Państwa organizacji do pandemii COVID-19.
- Wdrożenie polityki wymuszającej stosowanie silnych haseł oraz, w miarę możliwości, dwuskładnikowego uwierzytelniania dla wszystkich kont użytkowników zdalnych, a w szczególności dla usługi Office365
- Dostarczenie wszystkim pracownikom wskazówek i porad na temat bezpiecznego korzystania z rozwiązań do pracy zdalnej oraz identyfikacji ataków phishingowych
- Zapewnienie, by wszystkie komputery i urządzenia pracowników posiadały najnowsze aktualizacje oprogramowania – w tym antywirusowego i zapory ogniowej.
- Uruchomienie linii wsparcia, telefonicznej lub w formie czatu, zapewniającej pracownikom łatwy dostęp do wsparcia technicznego oraz możliwość zgłoszenia kwestii związanych z bezpieczeństwem takich jak phishing
- Szyfrowanie danych przechowywanych na urządzeniach wykorzystywanych do zdalnej pracy z uwagi na ryzyko kradzieży
- Wyłącznie na urządzeniach do zdalnej pracy obsługi nośników USB i wdrożenie innych sposobów przesyłania danych, takich jak narzędzia do współpracy zespołowej.

Dodatkowo, należy upewnić się, że Państwa procesy finansowe wymagają od zespołów ds. finansów w organizacji potwierdzenia wszystkich zleceń dotyczących dużych transakcji w czasie pandemii COVID-19. Stosowanie dodatkowej weryfikacji, najlepiej telefonicznie lub przez wiadomość SMS, pomoże ochronić organizację przez zwiększonym ryzykiem ataków typu BEC (Business E-mail Compromise) i podszywaniem się cyberprzestępców pod kadrę zarządzającą.

Istotne jest zapewnienie, by wszystkie systemy i urządzenia wykorzystywane w organizacji posiadały najnowsze aktualizacje i poprawki bezpieczeństwa , włączając w to urządzenia używane do pracy zdalnej. Należy być przygotowanym na wzmożone zainteresowanie cyberprzestępców próbami wykorzystania luk w zabezpieczeniach systemów IT podczas trwania pandemii.

Ponadto, powinni Państwo upewnić się, że dla wszystkich systemów krytycznych dla działania firmy regularnie tworzone są kopie zapasowe i zapewniona jest ich integralność. Są to działania, które pomogą organizacji zabezpieczyć się na wypadek podwyższonego ryzyka ataków ransomware w czasie pandemii COVID-19.

Warto również, wspólnie z zespołem zarządzania kryzysowego w przedsiębiorstwie, zadbać o zapewnienie zapasowego środowiska do prowadzenia audio i wideokonferencji. Ta alternatywna platforma okaże się nieocenionym w wsparciem w wypadku ataku ransomware, który zaburzy ciągłość działania systemów IT w organizacji oraz zapewni dodatkową nadmiarowość, gdyby Państwa główny dostawca usług telekonferencyjnych miał problemy z przepustowością lub dostępnością środowiska.

Pandemia COVID-19 z pewnością wprowadzi znaczące zmiany w sposobie w jaki Państwa organizacja funkcjonuje i chroni się przed zagrożeniami.

W przypadku pytań lub potrzeby uzyskania dodatkowych porad, prosimy o kontakt.

Materiał jest tłumaczeniem broszury KPMG pt.: „COVID-19 Staying cyber secure" opublikowanej 19 marca 2020. Skład i modyfikacje treści w języku polskim KPMG w Polsce.

Kontakt

Michał Kurek
Partner
Doradztwo biznesowe,
Cyberbezpieczeństwo
T: +48 22 528 1369
E: michalkurek@kpmg.pl

Łukasz Staniak
Senior Menedżer
Doradztwo biznesowe,
Cyberbezpieczeństwo
T: +48 22 528 3452
E: lstaniak@kpmg.pl

Marcin Strzałek
Menedżer
Doradztwo biznesowe,
Cyberbezpieczeństwo
T: +48 22 528 1073
E: mstrzalek@kpmg.pl

Biura KPMG w Polsce

Warszawa
ul. Inflancka 4A
00-189 Warszawa
T: +48 22 528 11 00
F: +48 22 528 10 09
E: kpmg@kpmg.pl

Kraków
ul. Opolska 114
31-323 Kraków
T: +48 12 424 94 00
F: +48 12 424 94 01
E: krakow@kpmg.pl

Poznań
ul. Roosevelta 22
60-829 Poznań
T: +48 61 845 46 00
F: +48 61 845 46 01
E: poznan@kpmg.pl

Wrocław
ul. Szczytnicka 11
50-382 Wrocław
T: +48 71 370 49 00
F: +48 71 370 49 01
E: wroclaw@kpmg.pl

Gdańsk
al. Zwycięstwa 13a
80-219 Gdańsk
T: +48 58 772 95 00
F: +48 58 772 95 01
E: gdansk@kpmg.pl

Katowice
ul. Francuska 36
40-028 Katowice
T: +48 32 778 88 00
F: +48 32 778 88 10
E: katowice@kpmg.pl

Łódź
ul. Składowa 35
90-127 Łódź
T: +48 42 232 77 00
F: +48 42 232 77 01
E: lodz@kpmg.pl

mampytanie@kpmg.pl

KPMG Poland

kpmg.pl