COVID-19 „PALIWEM” DLA CYBERPRZESTĘPCÓW. KONIECZNE ZWIĘKSZONE INWESTYCJE W CYBERBEZPIECZEŃSTWO [WYWIAD]

„Hakerzy próbują wykorzystać sytuację związaną z COVID-19 do szukania nowych wektorów ataku” stwierdził Mariusz Kochański członek zarządu Veracomp. W trakcie rozmowy ekspert mówił o tym, jak pandemia koronawirusa wpływa na aktywność cyberprzestępców oraz jakie działania należy podjąć, aby zmniejszyć ryzyko cyberataków.

W okresie pandemii koronawirusa obserwujemy wzrost aktywności cyberprzestępców. Jak ona się przejawia? Jakie metody są najczęściej stosowane?

Zmiana w trybie pracy, czyli przejście na pracę zdalną przez niemal 90% pracowników w wielu firmach to również nowa szansa dla cyberprzestępców. W Veracomp z home office korzysta 95% pracowników - praktycznie poza osobami, zatrudnionymi w magazynie wszyscy pracujemy zdalnie. Rzeczywistość wymusiła na nas bardzo szybkie przejście do tego modelu i dlatego nie mieliśmy dużo czasu na odpowiednie przygotowania.

Hakerzy stosując stare metody, próbują wykorzystać sytuację związaną z COVID-19 do szukania słabych punktów i wektorów ataku. Kontekst obecnej sytuacji spowodował, że mogą one być szczególnie skuteczne. Po pierwsze, wszyscy ogłosili śmierć bezpieczeństwa perymetrycznego, a należy pamiętać, że środowisko firmowe jest bezpieczniejsze niż środowisko domowe. Drugą ważną kwestią jest aspekt socjotechniczny związany z wirusem. Postępująca epidemia koronawirusa, która stała się problemem globalnym, spowodowała wzrost zainteresowania użytkowników tą tematyką. Zaczęli oni szukać w internecie informacji o zasadach zabezpieczenia się, możliwych lekach czy kwarantannie.

Dlaczego te kwestie są tak istotne? Phishing, spam i złośliwe oprogramowanie występowały przecież od zawsze, czyli od kiedy przenieśliśmy nas i biznes do sieci. Przez lata jednak wzrastała odporność ludzi na znane i popularne maile phishingowe. Chyba każdy zna przykład z wiadomością od prawnika z Nigerii o odziedziczonym spadku, który potrzebował jedynie przelewu na 10 tys. dolarów, aby dokończyć procedury. Wszyscy wiedzą już, że jest to oszustwo. Edukowanie ludzi w zakresie tego, co jest informacją prawdziwą, a co fałszywą w wiadomościach e-mail, które otrzymują każdego dnia na swoją skrzynkę, nie jest prostą sprawą. Zwłaszcza w tak elektryzującym temacie, jak COVID-19. Dlatego równolegle z walką ze skutkami pandemii powstał również drugi front działań mających na celu edukowanie użytkowników w jaki sposób rozpoznać e-maila przygotowanego w celu zainfekowania sprzętu złośliwą zawartością.

Jakie są konsekwencja dla bezpieczeństwa wynikające ze zmiany trybu pracy?

Niestety sieć domowa często jest nieodpowiednio zabezpieczona. Mnóstwo ludzi zostaje przy

domyślnych hasłach albo w ogóle ich nie stosuje. Dopóki używamy internetu domowego w celach rekreacyjnych, a nie do przetwarzania szczególnie istotnych danych, to głównym zagrożeniem jest to, że z naszą siecią połączy się sąsiad. Jeśli jednak do takiej niezabezpieczonej sieci podłączy się komputer firmowy i rozpocznie regularną pracę przez 8 godzin dziennie to haker zastaje niemal perfekcyjne okoliczności do ataku i idealne warunki do tego, aby w regularny sposób nasłuchiwać, co dzieje się w takiej sieci.

Kolejny problem związany z pracą w domu wiąże się z koniecznością drukowania firmowych dokumentów.. Integracja komputera służbowego z drukarką domową stwarza wysokie prawdopodobieństwo, że połączenie nie będzie odbywać się przez kabel, ale za pośrednictwem istniejącej sieci domowej, która nie należy do najbezpieczniejszych. Generuje ona zupełnie inny ruch, który nie będzie odbywał się przez VPN-a, dlatego połączenie będzie narażone na podsłuch czy ataki.

A bezpieczeństwo routerów domowych?

Najczęściej routery domowe są prekonfigurowane przez domyślnego dostawcę Internetu. Ataków na routery domowe wykorzystujące podatność CPE było naprawdę dużo. O ile dostawcy Internetu ze szczebla Tier 1, czyli operatorzy narodowi posiadają CERTy czy SOC i potrafią w porę dostrzec zagrożenia to sytuacja wygląda inaczej w przypadku, kiedy mamy do czynienia z mniejszymi firmami, konkurującymi ze sobą cenowo. W związku z tym skupiają się tylko na zapewnieniu nieprzerwanej i niezakłóconej łączności, zaniedbując bezpieczeństwo. Nie mogą też przypisać jednego eksperta jako osoby odpowiedzialnej tylko za dbanie o bezpieczeństwo.

Router domowy może mieć także własne podatności wynikające z wady produktów. Jeśli nawet zostały one wcześniej wykryte to niekoniecznie musiały zostać usunięte. A nawet jeśli producent patcha opublikował zmiany, użytkownik mógł zignorować konieczność wgrania odpowiedniej łatki. Większość wykorzystywanych routerów to proste i tanie urządzenia, które nie mają wyrafinowanych zabezpieczeń. Trzeba też pamiętać, że wiedza większości użytkowników na temat bezpieczeństwa jest niewielka i jeżeli operator nie zaktualizuje ich zdalnie to użytkownik pewnie sam tego nie zrobi. Czasami nie trzeba nawet atakować, ponieważ wiele sieci domowych nie ma żadnego hasła.

Mamy też drugą grupę użytkowników - tzw. power users, którym zależy na spersonalizowaniu opcji posiadanego routera i zarządzaniu nim zdalnie z internetu. Otwierają porty administracyjne lub stwarzają sobie możliwość logowania przez serwis webowy, co rodzi dodatkowe ryzyko. Może się np. zdarzyć, że haker wcale nie musi włamywać się do sieci, wystarczy mu dobrze przeskanowany router od strony portu LAN, żeby dowiedzieć się, jak zalogować się na konsolę administratora, z której można poustawiać bardzo wiele rzeczy.

Innym problemem jest również to, że ludzie mieszkający np. w obrębie kawiarni chcą zaoszczędzić na Internecie i logują się do sieci publicznej. Obecnie punkty WiFi w takich obiektach, dla wygody klientów, pozbawione są jakiegokolwiek hasła. Jednak warto pamiętać, że nigdy nie mamy pewności czy faktycznie logujemy się do sieci kawiarnianej. Równie dobrze może to być fałszywy access point.

Ostatnio dużym zainteresowaniem mediów cieszy się zjawisko tzw. zoombombingu. Jakie zagrożenie dla użytkownika niesie ze sobą to zjawisko?

Zoombombing to przykład tzw. video bombing związanym z przejściem wielu firm na styl pracy oparty na telekonferencjach w celu realizacji spotkań służbowych. Zoom nie jest moim ulubionym programem, ale w kontaktach z vendorami muszą go stosować, bo dla nich jest to korporacyjny standard. Znam jednak wiele przypadków, kiedy oprogramowanie to jest używane przez firmy zajmujące się bezpieczeństwem. Sam producent Zooma zadeklarował, że w pełni bezpieczny będzie dopiero od 30 maja, ponieważ łatanie jego dziur wymaga kompleksowej i długiej pracy. Niestety nie

da się wykluczyć możliwości, że ktoś wykorzysta luki w tym programie, aby nasłuchiwać co się dzieje w mojej domowej sieci WiFi.

Jakie są najbardziej popularne cele, na które hakerzy orientują swoje działania w kontekście sytuacji, w której się obecnie znajdujemy?

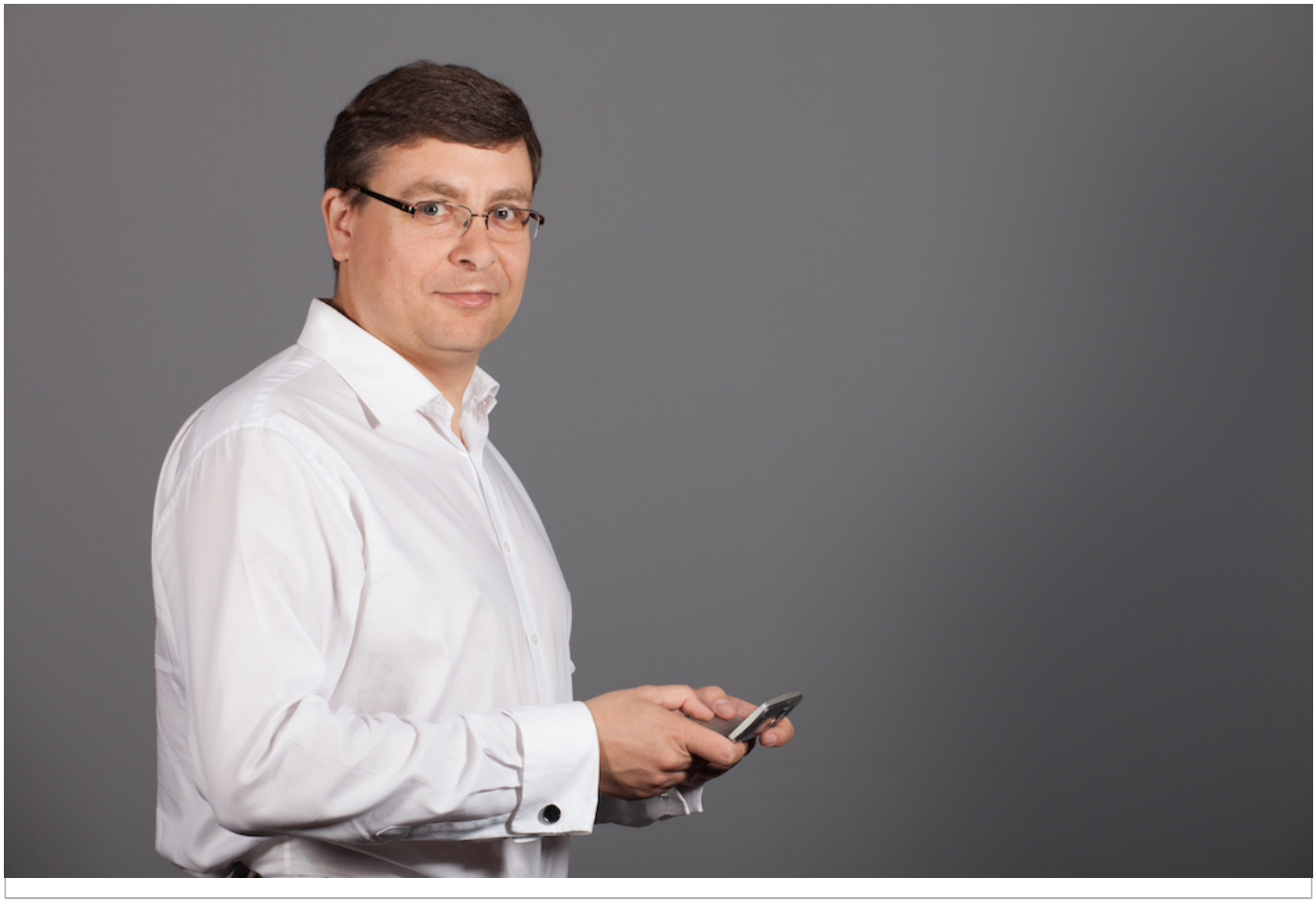
Jednym z wektorów ataku będzie phishing, a hakerzy będą podszywali się pod organizacje, które darzone są szczególnie dużym zaufaniem. W polskich warunkach przewidywałbym ataki na takie organizacje jak: Główny Inspektorat Sanitarny, Ministerstwo Zdrowia, lokalne sanepidy na poziomie wojewódzkim i powiatowym, szpitale, wojsko czy Policja.

Mówiąc o napastnikach możemy wskazać na nastolatków, którzy mają teraz więcej czasu - więc rekreacyjnie będą atakować różne cele, aby sprawdzić swoje umiejętności. Mamy również grupy hakerskie działające na zlecenie jakiegoś państwa, które działają w trybie ciągłym, a teraz będą wykorzystywać sytuację związaną z COVID-19 do realizacji długoterminowych celów politycznych swoich mocodawców. Pandemia koronawirusa osłabiła wszystkie kraje będące liderami politycznymi i gospodarczymi, co widać w szczególności w Stanach Zjednoczonych, ale również w Unii Europejskiej. Ta sytuacja polityczna i napięcia między państwami będą miały też odzwierciedlenie w zwiększonej liczbie cyberataków. Hakerzy, którzy chcą osłabić państwo atakują łańcuch dostaw: leków, benzyny, żywności, operatorów telekomunikacyjnych, media, sieci detaliczne czy farmaceutów.

Jeśli chodzi o cyberprzestępców szukających dodatkowe źródła dochodu, to największe pieniądze zarabia się hakując zarządy, ponieważ to na tym poziomie jest dostęp do największych zasobów finansowych. Wymaga to przygotowania takiego scenariusza ataku, żeby na samym końcu doprowadzić do realizacji przelewu. Nie zawsze to jednak oznacza, że celem hakerów będzie prezes wykorzystujący komputer służbowy w domu. Hakerzy mogą zaatakować innych szeregowych pracowników, żeby zobaczyć, jak są zbudowane zabezpieczenia w firmie i potem w oparciu o tożsamość tych pracowników przeprowadzić atak phishingowy na zarząd.

Obserwujemy też wzrost liczby ataków na szpitale czy instytucje medyczne. Takie ataki pojawiły się zarówno w Europie, u naszych sąsiadów Czechów, ale również w Stanach Zjednoczonych. Jaka jest pana opinia w tej sprawie - głupia zabawa, czy próba osłabienia państwa?

Nie można wykluczyć, że jest grupa osób, która uprawia tzw. hacking rekreacyjny. Bardziej prawdopodobny jest jednak scenariusz zakładający ataki hakerów pracujących na zlecenie państwa. W przypadku placówek medycznych znajdujących się w epicentrum pandemii, prawdopodobieństwo na zapłacenie okupu jest większe. W Polsce jest to jednak mało prawdopodobne, ponieważ szpitale nie mają środków, aby takie środki finansowe przekazać.



Jakie działania powinien podjąć biznes, ale również indywidualni użytkownicy, aby zminimalizować ryzyko ataku?

W przypadku firm sprawa jest prosta. Nie ważne jak świetnego eksperta posiada i ile wydaje na rozwiązania bezpieczeństwa - najsłabszym elementem zawsze będzie człowiek, czyli pracownik. Należy zacząć od edukacji. Jej brak może prowadzić do niebezpiecznych sytuacji, w których loginy i hasła będą zapisane na karteczkach przyklejanych do monitorów. Wprowadzenie zabezpieczeń jest najczęściej odbierane przez użytkowników jako utrudnianie im pracy. W firmach następują jednak pozytywne zmiany. Zaczynają one korzystać z pojedynczego logowania (przyp. red. możliwość jednorazowego zalogowania się do usługi sieciowej i uzyskania dostępu do wszystkich autoryzowanych zasobów zgodnych z tą usługą), haseł dynamicznych i uwierzytelnienia dwuskładnikowego. Najważniejsze są jednak odpowiednie szkolenia, ponieważ pracownicy muszą zrozumieć wagę problemu oraz poznać rzeczywiste skutki ataku hakera oraz realne szkody, jakie za sobą niosą. Muszą być uczuleni, że zaniedbania bezpieczeństwa mogą zakończyć się finansowymi stratami firmy, które doprowadzą do obniżenia ich pensji, a nawet zwolnień. Taki komunikat prezentujący skutki niewłaściwego zachowania będzie o wiele skuteczniejszy. Ważnym aspektem edukacji są też szkolenia przeciwko atakom socjotechnicznym, które wzmacniają świadomość pracowników, uzmysławiając im np. że ktoś może podszywać się pod informatyków firmowych czy dostawców oferujących pomoc.

Z jakimi zagrożeniami musimy się zmagać w naszych sieciach domowych?

Po raz kolejny konieczne jest przedstawienie negatywnych skutków niewłaściwego zachowania. Warto podkreślić, że brak zabezpieczeń sieci domowej może tak samo narazić dziecko na kontakt z pedofilem, jak i zakończyć się utratą kilku tysięcy złotych przez firmę, w której pracujemy. Istota

edukacji nie leży w treści, ponieważ podstawowe zasady są znane od lat, tylko w tym, żeby kluczowe standardy zostały zrozumiane, zapamiętane, a przede wszystkim stosowane. W tym celu muszą być one podane zrozumiałym językiem z ograniczeniem technicznego żargonu. Ponadto bardzo ważne są również motywacje odwołujące się do osobistych korzyści czy strat. Takie szkolenie musi być łatwe do zapamiętania np. poprzez powtarzanie kilku punktów, które są regularnie przypominane oraz tworzenie przykładów.

Musimy też uczulać użytkowników, żeby nie tworzyć prostych haseł. Mają w tym pomóc wprowadzane w systemach zasady, które uniemożliwiają akceptację łatwych do rozszyfrowania haseł, a także zmuszają użytkowników do ich regularnej aktualizacji oraz wprowadzania autoryzacji dwuskładnikowej.

Działania na rzecz poprawy bezpieczeństwa powinny być realizowane na pograniczu działu IT, HR i marketingu. W tym modelu dział marketingu pomaga informatykom stworzyć prosty, przyswajalny przekaz, ponieważ pracownicy działów IT mają z tym najczęściej duży problem. Kwestie HR też są bardzo ważne, ponieważ firma powinna określić jakie zasady bezpieczeństwa muszą znaleźć się np. w umowie o prace i regulaminach, a jakie powinny być w tzw. sferze miękkiej, odwołującej się do lojalności pracownika wobec firmy.

A VPNy? Jak ważne jest ich wykorzystywanie w firmie, a przede wszystkim jak powinna wyglądać polityka stosowania VPN-ów?

W momencie, w którym sytuacja zmusza nas do logowania się do systemów firmowych w sposób zdalny z innego miejsca niż biuro, VPN powinny być stosowane. Jeśli firma z nich nie korzysta, a udostępnia swoim pracownikom serwisy w sposób zdalny, powinna wdrożyć uwierzytelnienie przez certyfikat i HTTPS-a. Fizycznie wgrany certyfikat na służbowy sprzęt w połączeniu z HTTPS-em jest już jakąś formą dodatkowego zabezpieczenia. W międzyczasie, jeżeli przedsiębiorstwo korzysta z VPN-a, ze względu na wzrost liczby pracowników zdalnych powinno zwiększyć jego przepustowości. Przykładowo w amerykańskich bankach problem ten rozwiązano inaczej, wprowadzając logowanie w odpowiednich przedziałach czasowych.

Niedogodnością związaną ze stosowaniem VPN-a jest możliwość jego zbytniego przeciążenia np. kiedy pracownicy masowo zalogują się na wideokonferencję. W takiej sytuacji cały ruch internetowy odbywa się przez łącze internetowe firmy i ta wydajność przepustowości VPN-a będzie krytyczna. Do pracy zdalnej wystarczy kilkanaście kilobitów na sekundę, ale do wideo potrzebne jest już kilkaset kilobitów.

W standardowej, stacjonarnej pracy, firmy wykorzystywały w sieci biurowej SDN-y (programowalną sieć komputerową). W środowisku domowym wdrożenie takiego rozwiązania jest jednak mało prawdopodobne, z uwagi na brak kontroli nad routerem pracownika. Teoretycznie ten problem można byłoby rozwiązać poprzez wysłanie każdemu pracownikowi do domu skonfigurowanego routera, za pomocą którego mógłby się autokonfigurować, ale wiadomo, że w praktyce jest to niewykonalne.

Nie można też zapominać o sandboxingu i EDR (Endpoint Detection and Response – przyp. red.). Sandboxing, czyli mechanizm izolacji uruchamianych programów komputerowych od reszty systemu. Powinien zostać wdrożony z uwagi na urządzenia mobilne, które w ramach pracy zdalnej będą intensywniej wykorzystywane niż wcześniej. EDR to wschodzący trend wychodzący z założenia, że skoro nie można zabezpieczyć się przed wszystkimi zagrożeniami to EDR pozwoli nam odpowiednio wcześniej dowiedzieć się, co w kwestiach bezpieczeństwa dzieje się na służbowym komputerze pracownika.

Jakie działania użytkownik może podjąć, żeby zwiększyć bezpieczeństwo swojej sieci domowej?

Mamy zestaw podstawowych czynności. Pierwsza kwestia to odpowiedź na pytanie - jaki router w ogóle posiadam i jakie są jego zabezpieczenia. W tym celu możemy skorzystać z pomocy zespołu IT. Przykładowo na stronie Orange mamy bardzo ciekawe narzędzie - skaner podatności, który skanuje port routera, weryfikując zagrożenia. Korzystanie z niego nie wymaga specjalistycznej wiedzy informatycznej i nic nie kosztuje. Kolejny element to wprowadzenie sieci hasłowanej WiFi z WPA2 i z porządnym hasłem, które nie jest hasłem „słownikowym". Należy również zmieniać je przynajmniej raz w miesiącu. Jest jeszcze jedna ważna kwestia, czyli internet rzeczy. Ogólnie należy założyć, że im mniej urządzeń jest w sieci domowej tym lepiej. Dzisiaj największe niebezpieczeństwo nie płynie z komputerów tylko inteligentnych telewizorów, kamer IP czy czujników temperatury. Dlatego należy szukać rozwiązań, które umożliwią odseparowanie transmisji danych pomiędzy siecią domową, a telewizorem od reszty, ale bez pomocy ze strony IT jest to trudne.

Andrzej Kozłowski/Sylwia Gliwa

Materiał przygotowany we współpracy z Veracomp