Rekomendacje dotyczące bezpieczeństwa cybernetycznego

28-02-2022

EY
Building a better working world

1. Zarys sytuacji

Inwazja militarna na Ukrainę w połączeniu z wykorzystaniem cyberataków jako narzędzia walki stwarza duże prawdopodobieństwo, że firmy spoza Ukrainy mogą odczuć poważne skutki. Zwłaszcza jeśli ich centrale znajdują się w krajach nakładających sankcje na Rosję.

W kilku krajach sąsiadujących z Ukrainą odnotowano już ataki na mniejszą skalę na infrastrukturę[1] rządową i infrastrukturę[2] bezpieczeństwa. Możliwe są dalsze ataki.

Niektóre podmioty prowadzą długotrwałą, szeroko zakrojoną kampanię wymierzoną w zewnętrznych dostawców usług w zakresie przechowywania danych w chmurze, zarządzanych systemów informatycznych i innych usług w Stanach Zjednoczonych i Europie, aby umożliwić "dalszy" dostęp do klientów.

W celu przejęcia kont uprzywilejowanych dostawców usług, atakujący stosują szereg taktyk takich jak podszywanie się pod hasła, spear-phishing, kradzież tokenów i nadużywanie API.

- Wykorzystując skradzione dane uwierzytelniające, hackerzy dostają się do środowisk klientów.
- Wykorzystują pośrednie ścieżki i techniczne relacje zaufania, takie jak delegowane uprawnienia administracyjne (DAP), sieci VPN, niestandardowe rozwiązania dostępu do sieci oraz relacje na poziomie wielu dostawców.

W związku z powyższym kilka krajów podniosło swoje poziomy bezpieczeństwa (np. Polska przeszła na poziom Charlie-CRP, który stanowi niemal najwyższy poziom zagrożenia cybernetycznego).

2. Scenariusze zagrożeń I ryzyka

Biorąc pod uwagę trwający konflikt i impas dyplomatyczny na linii Rosja-NATO, dalsze ataki zakłócające lub niszczące oraz operacje informacyjne są wysoce prawdopodobne. Należy jednak zauważyć, że istnieje duża niepewność co do czasu i zakresu takich działań.

- Atakujący mogą przeprowadzać ataki poprzez narażanie na szwank łańcucha dostaw, tak jak w przypadku NotPetya w 2017 r. i SolarWinds w 2020 r., lub poprzez wykorzystanie znanych (np. Log4j) lub nieznanych ("zero-day") luk w zabezpieczeniach w celu uzyskania dostępu, rozprzestrzeniania się lub zakłócania działania.
- Organizacje poza Ukrainą mogą być narażone na bezpośrednie (tj. rozprzestrzenianie złośliwego oprogramowania przez Internet lub strony trzecie) lub pośrednie skutki. Przykładowo mogą to być regionalne zakłócenia w dostawach mediów, spedycji/logistyce, telekomunikacji lub innych usługach.
- Grupy przestępcze z siedzibą w Rosji mogą również nasilić ataki typu ransomware na organizacje zachodnie we wszystkich sektorach, w tym na obiekty infrastruktury krytycznej, których wybrane podmioty wcześniej unikały (np. szpitale, sektor naftowo-gazowy itp.).
- Chociaż celowe ataki na międzynarodowe firmy są mało prawdopodobne, możliwe są szkody uboczne spowodowane atakami zakłócającymi, w zależności od wektorów ataku.
- Biorąc pod uwagę historyczne wykorzystanie przez grupy rosyjskie niszczycielskich (np. NotPetya) i zakłócających ataków cybernetycznych (np. CrashOverride), atakujący niemal na pewno przeprowadzą podobne, szeroko zakrojone, niszczycielskie ataki poprzedzające działania wojskowe lub zbiegające się z nimi.
- Ataki takie będą miały na celu maksymalne zakłócenie funkcjonowania sektora cywilnego, w tym usług rządowych, użyteczności publicznej, transportu, usług finansowych i technologii; prawdopodobne są pośrednie skutki dla organizacji spoza Ukrainy.

[1] Reuters (Exclusive: Lithuania warns banks of cyber attacks, power cuts amid fears of war in Ukraine | Reuters)
[2] Reuters (Poland sees more cyberattacks on government servers, official says | Reuters)

3. Rekomendacje

Poniżej znajdują się zalecenia dla przedsiębiorstw i organizacji, a także kilka podstawowych zasad dla wszystkich użytkowników.

Dwie duże grupy hakerów (Anonymous i NB65) zadeklarowały, że Rosja i rosyjski rząd stały się ich głównym celem i w dniach 26 i 27 lutego 2022 r. przeprowadziły kilka udanych ataków. Jednocześnie niektóre organizacje (głównie finansowe) znajdują się w stanie podwyższonej gotowości z powodu decyzji politycznych i sankcji nałożonych na Rosję, ponieważ podejrzewają, że cyberataki będą odwetem.

- Rosyjska strona rządowa stała się nieosiągalna, włamano się do rosyjskiej telewizji państwowej, która pokazała inny kluczowy przekaz. Ponadto złamano zabezpieczenia rosyjskiej komunikacji wojskowej, która została następnie opublikowana.
- Prezydent Joe Biden uzyskał możliwość przeprowadzenia zmasowanego cyberataku w celu zakłócenia rosyjskich operacji wojskowych na Ukrainie. Nie wiadomo, kto miałby przeprowadzić atak (U.S. Cyber Command, Agencja Bezpieczeństwa Narodowego czy CIA). Na dzień publikacji niniejszych rekomendacji nie opublikowano żadnej publicznej decyzji w tej sprawie.
- Banki amerykańskie przygotowują się do odwetowych ataków cybernetycznych po nałożeniu najnowszych sankcji na Rosję (odcięcie od systemu SWIFT). Banki światowe zwiększają monitorowanie i przygotowują się na sponsorowane przez państwo ataki na instytucje finansowe.

4. Rekomendacje dla przedsiębiorców

Kluczowe działania natychmiastowe

- Konieczne jest przejrzenie konfiguracje i kontrole aktywów o dużej wartości, nadając im priorytet w oparciu o potencjalne skutki biznesowe.
- Administratorzy systemów powinni sprawdzić, czy wszystkie kopie zapasowe i kopie są odizolowane i nie ucierpią w przypadku ataku na całą infrastrukturę.
- Należy wyznaczyć osobę odpowiedzialną za koordynację działań w przypadku wystąpienia incydentu bezpieczeństwa. Jednocześnie należy przetestować w praktyce procedury reagowania w przypadku wystąpienia incydentu.
- Niezbędne jest zapewnienie ograniczenia i monitorowania ruchu wejściowego i wyjściowego w zależności od lokalizacji sieci i roli biznesowej.
- Ograniczenie i monitorowanie ruchu bocznego między środowiskami lokalnymi i zewnętrznymi oraz w ich obrębie, w tym w chmurach partnerów/dostawców jest niezbędne; należy być przygotowanym na całkowite odłączenie oddziałów.

Zalecenia długoterminowe

- Zaleca się przetestowanie możliwości odzyskiwania infrastruktury, czyli odtwarzania z kopii zapasowych. Należy to zrobić w praktyce, a nie tylko w ramach procedury.
- W zależności od stopnia narażenia, należy wstępnie przygotować dane, personel i zasoby, aby ułatwić płynne przejście do procedur ciągłości działania i przywracania z kopii zapasowych.
- Upewnij się, że solidna, wielopoziomowa polityka tworzenia kopii zapasowych, obejmująca rozproszone geograficznie kopie zapasowe w trybie on- i offline, funkcjonuje prawidłowo i jest należycie przećwiczona.
- Należy współpracować z interesariuszami z różnych jednostek i zespołów biznesowych w celu określenia bezpośrednich lub pośrednich powiązań/narażenia na oddziaływanie regionu Ukrainy, takich jak oprogramowanie pochodzenia ukraińskiego, operacje zagraniczne, usługodawcy zewnętrzni, sprzedawcy/dostawcy z lokalnymi biurami lub telepracownicy/kontrahenci.

- Zaleca się powołanie interdyscyplinarnego komitetu sterującego, który będzie informował o rozwoju sytuacji i wpływach oraz koordynował czas i sposób reakcji.
- Zidentyfikuj i wzmocnij zasoby posiadające dostęp do Internetu, aby chronić je przed nieautoryzowanym dostępem lub wykorzystaniem; załataj znane luki w zabezpieczeniach i zapewnij segmentację danych i sieci.
- Należy regularnie aktualizować całe oprogramowanie, zwłaszcza w przypadku wszystkich systemów podłączonych do Internetu. Aktualizację warto rozpocząć od systemów, w których występują powszechnie znane i aktywne luki wykorzystywane przez hakerów.
- Upewnij się, że dostęp do wszystkich danych organizacyjnych i sieci wewnętrznych wymaga uwierzytelniania wieloczynnikowego (MFA) i/lub RBAC dla wszystkich kont - w tym partnerów i kontrahentów - zwłaszcza tych bezpośrednio/pośrednio związanych z regionem.
- Należy dokonać przeglądu usług adresowych organizacji i ograniczyć je do niezbędnego minimum. Do tego celu można wykorzystać oprogramowanie, takie jak portal Shodan. Należy bezwzględnie zrezygnować z usług umożliwiających bezpośredni dostęp zdalny (np. RPD lub VNC).
- Sygnatury bezpieczeństwa wszystkich systemów (takich jak AV, EDR, IDS, IPS, itp.) powinny być automatycznie aktualizowane.
- Organizacja powinna zapoznać się z zaleceniami odpowiednich CERTS i przygotować się na ataki typu DDoS (Denial of Service) na swoją infrastrukturę.
- Administratorzy organizacji powinni stosować odpowiednie zalecenia i wytyczne CERTS, aby wzmocnić i wdrożyć zabezpieczenia przed oprogramowaniem ransomware.
- Należy przejrzeć i wdrożyć wszystkie wytyczne i zalecenia dotyczące bezpieczeństwa haseł i kodów dostępu.
- Zalecane jest wdrożenie mechanizmów identyfikacji nadawcy wiadomości dla wszystkich domen wykorzystywanych do wysyłania poczty. Komunikacja mailowa powinna być wzmocniona poprzez wdrożenie podpisywania i jeśli to możliwe - szyfrowania.
- Jeśli organizacja posiada lub korzysta z własnego zakresu adresów IP, zaleca się dodanie ich do platformy N6. Dzięki temu organizacja będzie posiadała aktualne informacje o podatnościach i złośliwych działaniach w obserwowanym zakresie.
- Pracownicy powinni zostać poinstruowani, aby obserwować i zgłaszać wszelkie dziwne lub złośliwe działania do wyznaczonej osoby odpowiedzialnej za zbieranie takich zgłoszeń.
- Należy wyznaczyć punkt kontaktowy (nawet jeśli lokalne prawo i przepisy tego nie wymagają), który będzie odpowiedzialny za komunikację z odpowiednim zespołem z lokalnego CERT. Przyspieszy to cały proces komunikacji i ułatwi specjalistom z CERT znalezienie potrzebnych pracowników w organizacji. Podejrzane działania powinny być zgłaszane do odpowiednich lokalnych zespołów CERT lub innych właściwych agencji.

5. Rekomendacje dla użytkowników indywidualnych

- Zachęcamy użytkowników do sprawdzania ustawień zabezpieczeń swoich kont pocztowych i kont w mediach społecznościowych.
- Użytkownicy powinni być ostrożni wobec wszelkich sensacyjnych wiadomości i informacji, zwłaszcza tych zachęcających do podjęcia szybkich działań. Takie informacje powinny być sprawdzone i zweryfikowane z co najmniej kilku źródeł. Użytkownicy muszą mieć pewność, że informacje są prawdziwe, zanim wyślą je do mediów społecznościowych. W przypadku jakichkolwiek wątpliwości, użytkownik powinien wstrzymać się z podjęciem wszelkich działań.
- Użytkownicy powinni zwracać uwagę na wszelkie hiperłącza w wiadomościach e-mail i SMS - zwłaszcza te, które zachęcają do podjęcia szybkich działań (zmiana hasła, podejrzana aktywność na koncie). W przeszłości wiele ataków na konta prywatne stanowiło furtkę do ataku na organizację.

- Użytkownicy powinni tworzyć kopie zapasowe ważnych plików i być w stanie odzyskać te pliki w razie potrzeby.
- Użytkownicy powinni być świadomi wiadomości i ostrzeżeń o nowych atakach, czytając okresowo portale bezpieczeństwa i alerty w mediach społecznościowych.

EY | Building a better working world

Celem działalności EY jest budowanie lepiej funkcjonującego świata - poprzez wspieranie klientów, pracowników i społeczeństwa w tworzeniu trwałych wartości - oraz budowanie zaufania na rynkach kapitałowych.

Wspomagane przez dane i technologię, zróżnicowane zespoły EY działające w ponad 150 krajach, zapewniają zaufanie dzięki usługom audytorskim oraz wspierają klientów w rozwoju, transformacji biznesowej i działalności operacyjnej.

Zespoły audytorskie, consultingowe, prawne, strategiczne, podatkowe i transakcyjne zadają nieoczywiste pytania, by móc znaleźć nowe odpowiedzi na złożone wyzwania, przed którymi stoi