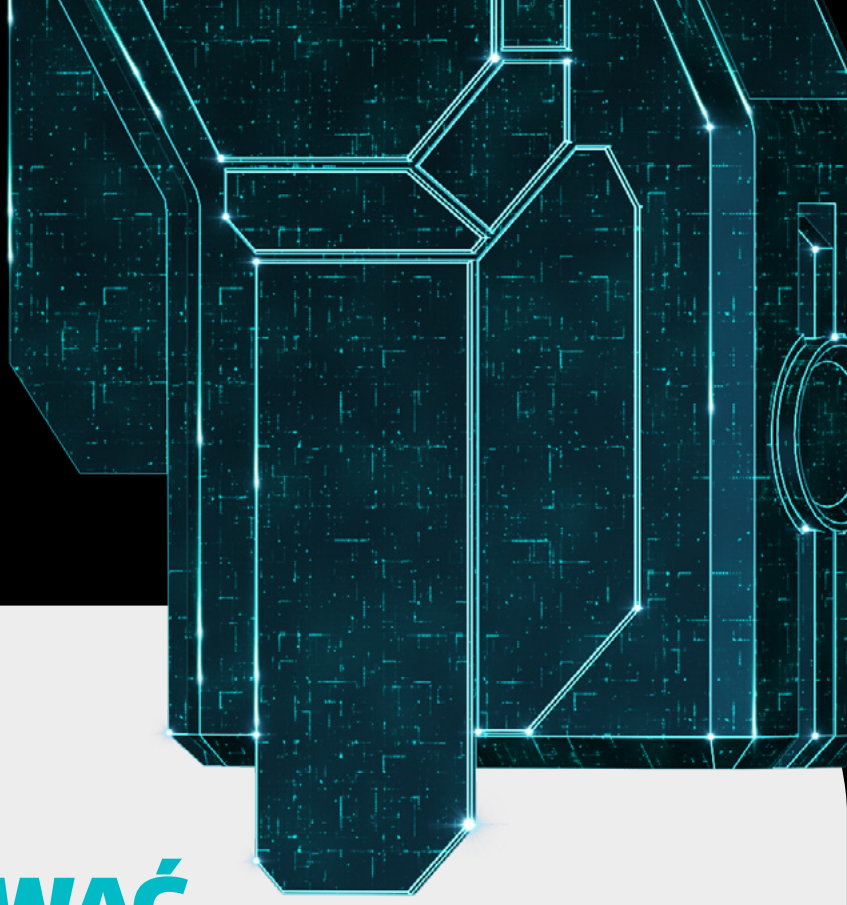
CYBERSECURITY
EXPERTS ON YOUR SIDE



RDP: JAK SKONFIGUROWAĆ ROZWIĄZANIA BEZPIECZEŃSTWA Z MYŚLĄ O PRACY ZDALNEJ

Korzystasz z RDP do zarządzania firmową siecią w trakcie kryzysu? W takim razie zadbaj o to, by zminimalizować ryzyko dzięki dobrym praktykom, narzędziom do uwierzytelniania oraz poprzez wykorzystanie posiadanej wiedzy.

Pandemia koronawirusa zmusiła firmy na całym świecie, by wysłały swoich pracowników do domu oraz wdrożyły pracę zdalną tam, gdzie to tylko możliwe. To oznacza, że do łask wkroczyła także technologia RDP, która w ciągu minionych lat wielokrotnie była nadużywana przez cyberprzestępców. Stała się ona źródłem szeregu incydentów, szczególnie tam, gdzie przestępcy byli w stanie wykorzystać błędnie skonfigurowane zabezpieczenia oraz słabe hasła, by uzyskać dostęp do firmowych sieci. Po włamaniu mogli zrobić w zasadzie wszystko, np. dokonać kradzieży własności intelektualnej oraz innych wrażliwych danych lub zaszyfrować firmowe pliki dla okupu.

AUTOR:Aryeh Goretsky
WKŁAD MERYTORYCZNY: James Shepperd

Kwiecień 2020

1.

1. Jak atakujący wykorzystują RDP?

W ciągu ostatnich kilku lat ESET zidentyfikował szereg incydentów, w których przestępcy łączyli się przez Internet z serwerami z systemem Windows za pośrednictwem protokołu RDP, a następnie logowali się jako administrator. Sugeruje to jeden z kilku wektorów ataku, w tym wykorzystanie istniejących podatności (np. BlueKeep CVE-2019-0708), phishing, credential stuffing, password spraying, brute force lub błąd w konfiguracji dostępu do wewnętrznych systemów.

Kiedy napastnicy są już zalogowani na serwerze jako administrator, ich następnym krokiem jest najczęściej przeprowadzenie podstawowego rekonesansu. Ma on na celu ustalić do czego jest wykorzystywany dany komputer, przez kogo i kiedy. Kiedy już mają te informacje, rozpoczynają się właściwe działania.

Poniższa lista nie wymienia wszystkich aktywności, które cyberprzestępcy mogą zrealizować, ani nie oznacza, że są one wykonywane przy każdym ataku. Przebieg każdego incydentu i kroki podejmowane przez hakerów różnią się znacząco w zależności od okoliczności.

CZĘSTE ZŁOŚLIWE AKTYWNOŚCI OBEJMUJĄ:

- usuwanie plików z logami, zawierającymi dane na temat włamania
- wyłączanie zaplanowanych operacji tworzenia kopii zapasowych
- wyłączanie oprogramowania antywirusowego lub tworzenie w nim wyjątków (co może zrobić wyłącznie administrator)
- pobieranie i instalowanie różnych programów na serwerze
- usuwanie lub nadpisywanie starych backupów, jeśli są dostępne
- wykradanie danych z serwera

TRZY NAJBARDZIEJ POPULARNE ZŁOŚLIWE AKTYWNOŚCI TO:

- instalacja oprogramowania wydobywającego kryptowaluty, np. Monero
- instalacja ransomware w celu wymuszenia na organizacji okupu, opłacanego zwykle w kryptowalutach
- w wybranych przypadkach przestępcy mogą zainstalować dodatkowe oprogramowanie, ułatwiające im zdalny dostęp do urządzenia, nawet jeśli ich aktywność związana z RDP zostanie wykryta i zablokowana

ZNANE PRZYKŁADY WYKORZYSTANIA RDP W ATAKACH

Jeden z bardziej skutecznych wirusów szyfrujących, GandCrab, aktywny do maja 2019, funkcjonował w ramach modelu biznesowego Ransomware-as-a-Service. Oznacza to, że twórcy wirusa nie dystrybuowali go sami, a zajmowali się tym inni przestępcy, gotowi za niego zapłacić. Był on wykorzystywany przede wszystkim przeciwko dostawcom usług zarządzanych (MSP) i wykorzystywał RDP by łączyć się z ich zdalnymi narzędziami zarządzania, a następnie wyłudzać okup od kilku ofiar jednocześnie.

Operatorzy wirusa GrandCrab ogłosili, że kończą swoją działalność po tym, jak FBI opublikowało klucze, pozwalające ich ofiarom odszyfrować swoje pliki. Kod źródłowy wirusa został jednak najprawdopodobniej sprzedany innej grupie. Ta odpowiada aktualnie za ransomware Sodinokibi, który charakteryzuje się względem poprzednika szeregiem zmian w kodzie, strukturze i licznymi usprawnieniami. Sodinokibi pojawiło się krótko po zawieszeniu działalności grupy odpowiedzialnej za GrandCrab, stając się w praktyce jego następcą. Wirus wykorzystywał bardzo podobne taktyki, techniki i procedury co jego poprzednik, biorąc na cel dostawców usług zarządzanych z wykorzystaniem protokołu RDP.

Ataki wymierzone w firmy świadczące usługi MSP powinny zaniepokoić także inne organizacje, ponieważ to właśnie one posiadają "klucze do królestwa", gwarantujące dostęp do tysięcy małych, a nawet części dużych korporacji. Klienci MSP są z kolei postawieni w sytuacji, gdzie bez ich pomocy nie są w stanie skutecznie zarządzać wykorzystywanymi w firmie rozwiązaniami bezpieczeństwa – podobnie jak użytkownicy bez wsparcia administratorów.

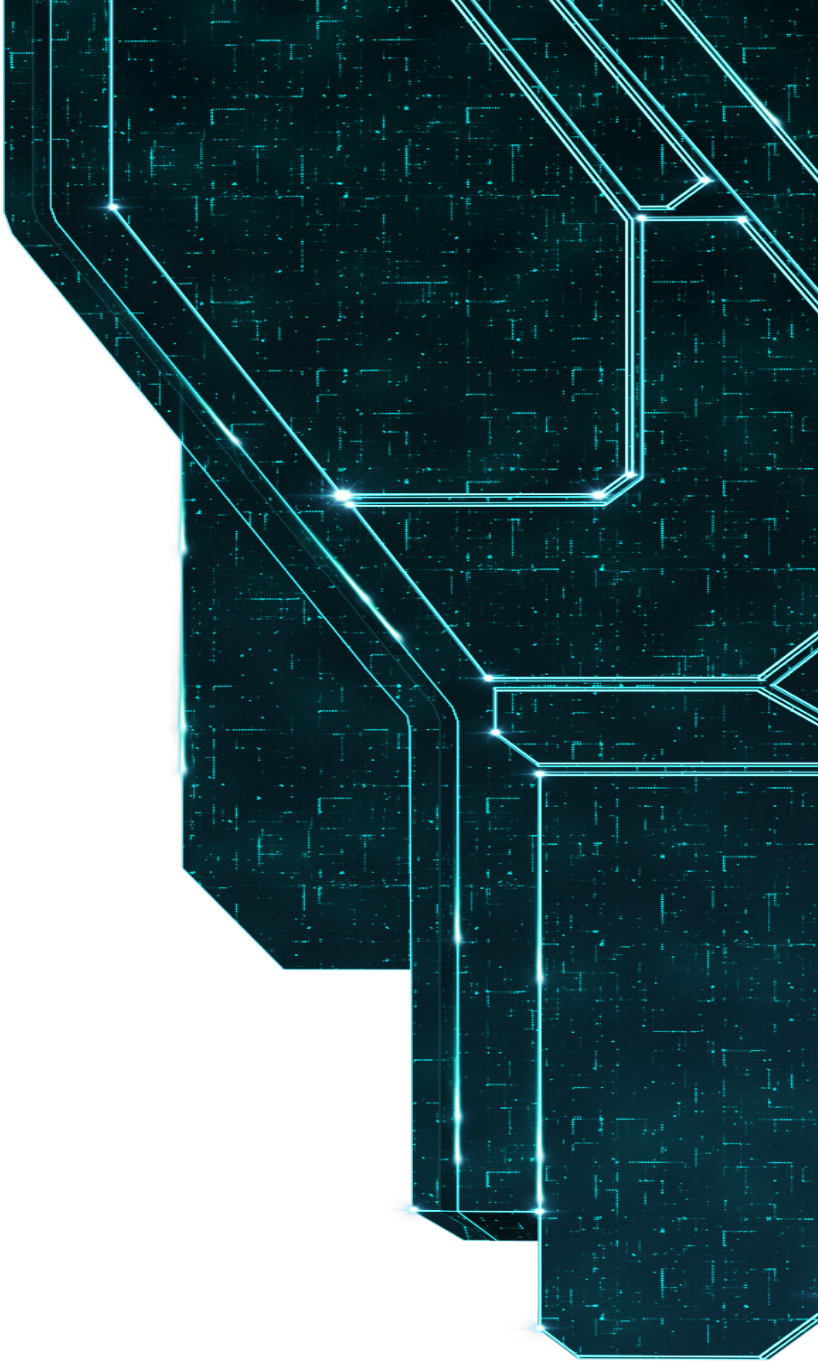
PODATNOŚCI W RDP TO OLBRZYMIA FURTKA DLA PRZESTĘPCÓW

Ataki z wykorzystaniem RDP powoli, acz sukcesywnie zyskują na popularności. Stały się w związku z tym przedmiotem szeregu wytycznych ze strony m.in. FBI, brytyjskiego NCSC, kanadyjskiego CCCS oraz australijskiego ACSC.

W maju 2019 na światło dzienne trafiły informacje o podatności CVE-2019-0708, tzw. „BlueKeep", zagrażającej komputerom z systemami Windows 2000 , Windows XP, Windows Vista, Windows 7, Windows Server 2003, Windows Server 2003 R2, Windows Server 2008 oraz Windows Server 2008 R2*.

Choć w większości mowa tu o starszych, niewspieranych już w wersjach systemów operacyjnych, zgromadzone przez nas dane telemetryczne sugerują, że wiele z nich nadal jest w użyciu.

Luka BlueKeep umożliwia napastnikom uruchomienie dowolnego kodu na komputerze ofiary. Nawet pojedynczy atakujący może z jej pomocą wyrządzić szkody na szeroką skalę, wykorzystując w tym celu narzędzia do automatyzacji. Prawdziwe zagrożenie wynika jednak z faktu, że złośliwe oprogramowanie może rozprzestrzeniać się z pomocą luki bez żadnego udziału ze strony użytkownika. Można to było zaobserwować m.in. przy okazji wirusów Win32/Diskcoder.C (NotPetya) i Conficker.



ESET OFERUJE DARMOWE NARZĘDZIE, POZWALAJĄCE ZIDENTYFIKOWAĆ SYSTEMY ZAGROŻONE PODATNOŚCIĄ BLUEKEEP (CVE-2019-0708). PLIKI INSTALACYJNE WRAZ Z INSTRUKCJĄ OBSŁUGI ZNAJDZIESZ POD PONIŻSZYM LINKIEM.

ZOBACZ ARTYKUŁ

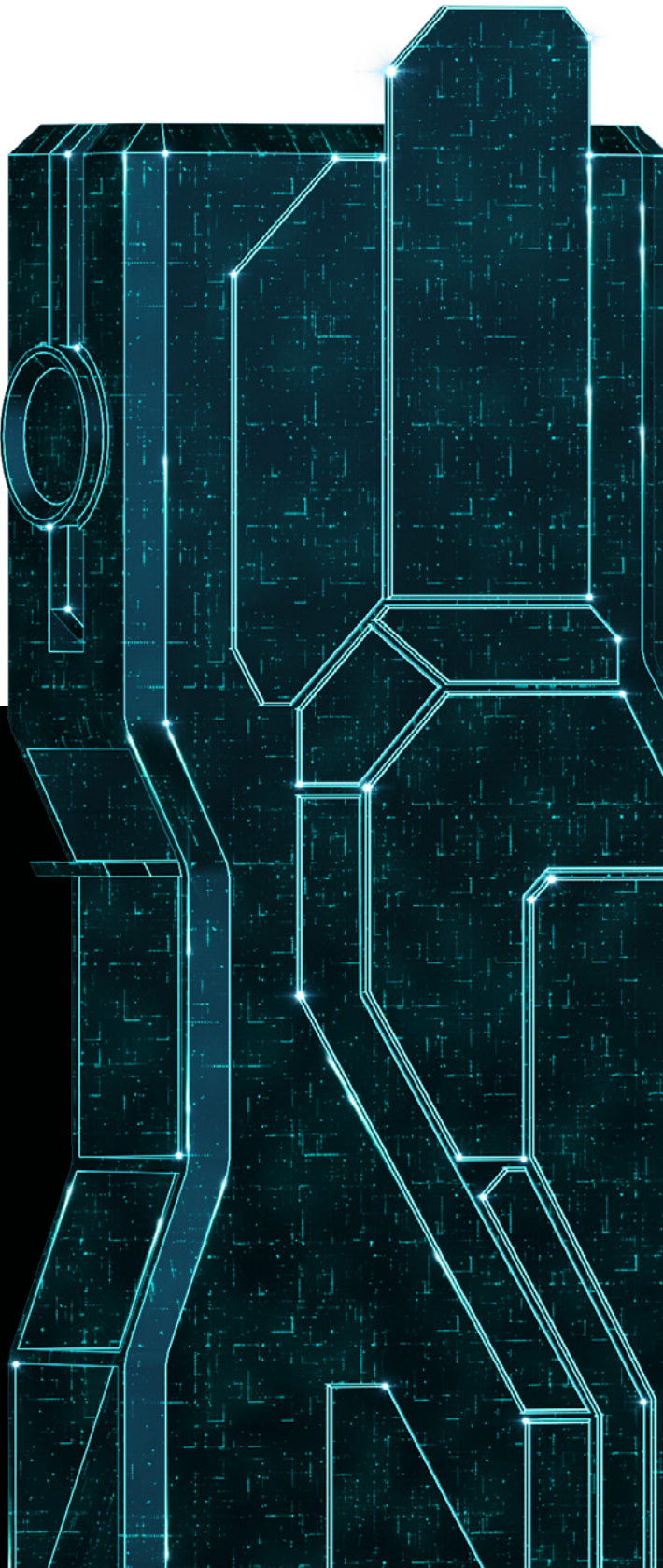
Materiał w języku angielskim

Uwaga*: *Zgodnie z wiedzą na dzień pisania artykułu, systemy Windows 8, Windows Server 2012 i nowsze nie są zagrożone.*

Możliwość wykorzystania przez cyberprzestępców tego typu podatności stanowi poważny problem. Microsoft w swoich zaleceniach dla klientów przydzielił jej najwyższy możliwy wskaźnik ważności, „Krytyczna", natomiast w prowadzonej przez rząd USA National Vulnerability Database posiada ona rangę 9.8 na 10. Microsoft opublikował post na swoim blogu, w którym zaleca, by użytkownicy zainstalowali najnowsze łatki bezpieczeństwa także na niewspieranych systemach, takich jak Windows XP czy Windows Server 2003. Obawy o możliwość wykorzystania podatności przez cyberprzestępców były na tyle poważne, że w czerwcu 2019 amerykańska agencja NSA opublikowała nietypowe dla siebie zalecenia, by zainstalować wydane przez Microsoft łatki.

Choć luka BlueKeep cieszyła się dużą popularnością wśród instytucji zajmujących się testami penetracyjnymi, aż do listopada 2019 roku rzadko była wykorzystywana w realnych atakach. Nagły wzrost aktywności można było zaobserwować dopiero w listopadzie 2019, kiedy masowo zaczęły się pojawiać doniesienia o incydentach z jej udziałem, jak donoszą serwisy ZDNet i WIRED. Ataki miały być w zdecydowanej większości nieskuteczne – 91% podatnych komputerów przestawało działać, zgłaszając jednocześnie komunikat błędu (tzw. „Niebieski Ekran Śmierci", BSOD) w momencie wykorzystania BlueKeep przez napastnika. W przypadku pozostałych 9% przestępcom udało się zainstalować na komputerach oprogramowanie kopiące kryptowalutę Monero. Choć nie był to samorozprzestrzeniający się atak, którego wszyscy się obawiali, odpowiedzialnej za niego grupie udało się zautomatyzować cały proces, choć z niewielką skutecznością.

Żeby jednak nie tracić czasu, zamiast szczegółowo opisywać samą podatność skupimy się na krokach, które należy podjąć, żeby chronić swoją sieć przed zagrożeniem.



2.

2. Ochrona przed napastnikami korzystającymi z RDP

Co w takim razie można zrobić, żeby zabezpieczyć się przed atakami z wykorzystaniem RDP? Przede wszystkim przestać łączyć się za jego pomocą przez Internet bezpośrednio ze swoimi serwerami, a przynajmniej ograniczyć takie sytuacje do niezbędnego minimum. Dla wielu firm może się to okazać problematyczne, szczególnie teraz, kiedy wielu pracowników pracuje z domu, często w warunkach kwarantanny.

Trzeba jednak podkreślić, że jeśli nadal korzystasz z systemów Windows Server 2008 i Windows 7 (które nie są już wspierane od stycznia 2020) na maszynach, z którymi można się połączyć za pośrednictwem RDP, jesteś narażony na atak i powinieneś natychmiast podjąć środki zaradcze. Korzystanie z tych platform znacząco zmniejsza poziom bezpieczeństwa, w związku z czym zanim wdrożysz poniższe porady, koniecznie zadbaj o ich zaktualizowanie do jednej z nadal wspieranych wersji.

W przypadku komputerów z aktualnym oprogramowaniem sytuacja nie wymaga natychmiastowej rezygnacji z RDP, choć należy podjąć dodatkowe kroki, by zabezpieczyć je tak szybko i dokładnie, jak to tylko możliwe. W tym celu stworzyliśmy tabelę, gdzie wskazujemy 12 kroków, które należy podjąć, by skutecznie zabezpieczyć się przed atakami z wykorzystaniem RDP.

12 REKOMENDACJI JAK ZABEZPIECZYĆ RDP

Rady w poniższej tabeli zostały uszeregowane w oparciu o ich znaczenie i łatwość implementacji, które mogą się różnić w zależności od organizacji. Część z nich może nie mieć zastosowania lub lepiej będzie je wdrożyć w innej kolejności; może się także pojawić konieczność wdrożenia dodatkowych kroków.

	REKOMENDACJA	POWÓD
1	Zablokuj wszystkie połączenia do lokalnych komputerów na porcie 3389 (TCP/UDP) na firewallu brzegowym.*	Całkowicie blokuje dostęp do RDP przez Internet.
2	Przetestuj i wdróż łatki dla podatności CVE-2019-0708 (BlueKeep) i włącz uwierzytelnianie na poziomie sieci.	Instalacja łatek dostarczonych przez Microsoft i przestrzeganie załączonych rekomendacji bezpieczeństwa pomaga chronić urządzenia przed podatnością BlueKeep.
3	Dla wszystkich kont mogących zalogować się przez RDP wymagaj złożonych haseł (silne hasło zawierające przynajmniej 15 znaków, bez powiązań z firmą, oferowanych produktów lub danego użytkownika).	Chroni przeciwko atakami polegającymi na zgadywaniu haseł i atakach typu credential stuffing. Proces można łatwo zautomatyzować, a wzrost długości haseł znacząco wpływa na ich skuteczność.
4	Chroń dostęp do serwerów za pomocą unikalnych haseł dla lokalnych kont z uprawnieniami administratora (np. używając LAPS lub sprawdzonego menedżera haseł) **Dodatkowo: Ogranicz liczbę użytkowników mających do nich dostęp*	*(jak powyżej)* Ogranicza powierzchnię ataku w przy-padku serwerów, zmniejszając liczbę użytkowników, którzy mogą uzyskać do nich dostęp.
5	Ustaw poziom szyfrowania klienckich połączeń RDP na "wysoki", jeśli to możliwe. Jeśli nie, skorzystaj z najwyższego dostępnego poziomu szyfrowania.	Korzysta ze 128-bitowego szyfrowania dla całej komunikacji klient-serwer tam gdzie to możliwe.

6	Zainstaluj rozwiązanie wieloskładnikowego uwierzytelniania, takie jak ESET Secure Authentication (ESA). Wymagaj wieloskładniko-wego uwierzytelniania w przypadku wszystkich kont, do których można się zalogować za pośrednictwem RDP oraz kont administratora.	Wymaga dodatkowej warstwy uwierzytelniania dostępnej wyłącznie dla użytkowników, wymagającej skorzystania z urządzenia mobilnego, specjalnego tokenu sprzętowego lub jednorazowego hasła podczas logowania się na urządzenie.
7	Wymagaj połączenia VPN w przypadku wszystkich połączeń RDP spoza lokalnej sieci.	Uniemożliwia połączenie RDP z Twoją lokalną siecią z Internetu. Umożliwia wdrożenie silniejszych mechanizmów związanych z identyfikacją i uwierzytelnianiem użytkownika w przypadku zdalnego dostępu do komputerów.
8	Upewnij się, że wszystkie rozwiązania bezpieczeństwa, do których dostęp chroniony jest hasłem, wykorzystują silne hasła, które nie mają związku z kontem administratora ani innymi kontami usług. ESET Security Management Center (ESMC) umożliwia łatwe, granularne zarządzanie politykami dla różnych grup użytkowników. Dodatkowo ESMC pozwala na obsługę wielu użytkowników i umożliwia zabezpieczenie dostępu za pomocą uwierzytelniania wieloskładnikowego.	Zapewnia dodatkową warstwę ochrony w sytuacji, gdyby atakujący próbował przejąć konto administratora.
9	Włącz ochronę przed podatnościami w oprogramowaniu firm trzecich w swoim rozwiązaniu bezpieczeństwa dla stacji roboczych, która będzie monitorować działanie często atakowanych aplikacji.	Wiele programów do ochrony stacji roboczych gwarantuje ochronę przed atakami z wykorzystaniem podatności. Upewnij się, że jest włączona.
10	Wyizoluj wszystkie niezabezpieczone komputery, które muszą mieć zagwarantowany dostęp przez RDP.	Izolacja pozwoli zablokować dostęp do reszty firmowej sieci z poziomu podatnych komputerów.
11	Wymień komputery z niewspieranym systemem operacyjnym.	Jeśli na jakimkolwiek komputerze w sieci nie można zainstalować łatki chroniącej przed BlueKeep, zaplanuj jego wymianę.
12	Rozważ wdrożenie blokady połączeń w oparciu o geolokację.	Jeśli wszyscy pracownicy i dostawcy usług znajdują się w tym samym kraju albo w wąskiej grupie państw, zablokowanie dostępu z innych lokalizacji pomoże ochronić sieć przed atakami zza granicy.

***Domyślnie RDP działa na porcie 3389.** *Jeśli zmieniłeś go na inny, to jego należy zablokować.*

3.

Jak ESET pomaga chronić RDP?

Jako pierwszy krok warto się upewnić, że wykorzystywane rozwiązanie do ochrony stacji roboczych jest: a) zaktualizowane do najnowszej wersji oraz b) wykrywa i chroni przed podatnością BlueKeep. Dopiero wtedy można się skupić na bardziej szczegółowych działaniach związanych z konkretnymi warstwami bezpieczeństwa. Moduł ochrony przed atakami z sieci, dostępny w produktach ESET od wersji 7 wzwyż jako rozszerzenie funkcji firewall, wykrywa BlueKeep jako CVE-2019-0708.

Kolejną technologią kluczową w kontekście ochrony przed RDP jest ESET Exploit Blocker, który monitoruje najczęściej atakowane przez atakujących aplikacje (przeglądarki internetowe, czytniki dokumentów, aplikacje pocztowe, Flasha, Javę i inne). Zamiast skupiać się na konkretnych identyfikatorach CVE, zagrożenia są identyfikowane w oparciu o konkretne techniki wykorzystywane w ataku. W przypadku wykrycia zagrożenie jest natychmiast blokowane na poziomie danego urządzenia.

Obok technologii istotne jest jednak wdrożenie odpowiednich procesów, które powinny być przyjazne dla użytkownika oraz oparte o proste w użyciu narzędzia. Skuteczne zabezpieczenie RDP wymaga kilku kroków, przy czym proste w użyciu rozwiązanie wieloskładnikowe uwierzytelniania (MFA) wydaje się tutaj najbardziej kluczowym elementem, ponieważ funkcjonuje jako główna linia obrony przed ryzykiem złamania prostych do odgadnięcia haseł. Skupiając się na procesie uwierzytelniania, w tym przypadku podczas logowania do RDP, ochronie podlega jeden z kluczowych systemów związanych z zarządzaniem bezpieczeństwa sieci oraz użytkowników.

ESET Secure Authentication, rozwiązanie MFA firmy ESET, chroni kluczową komunikację, w tym Remote Desktop Protocol, poprzez wdrożenie dodatkowego składnika uwierzytelniania.

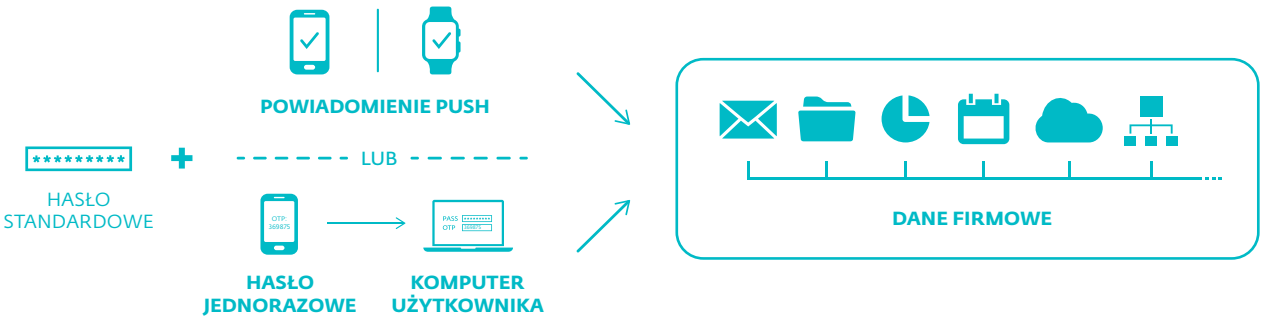
ESET Secure Authentication może chronić wszystkie rozwiązania VPN (które same w sobie stanowią jeden z kluczowych elementów zapewnienia bezpieczeństwa firmowych zasobów), proces logowania do kluczowych urządzeń, na których zgromadzone są poufne dane, a także do usług chmurowych, w tym Office 365, Google Apps, Dropbox i wielu innych. W tym celu wykorzystywane jest ADFS 3.0 lub SAML.

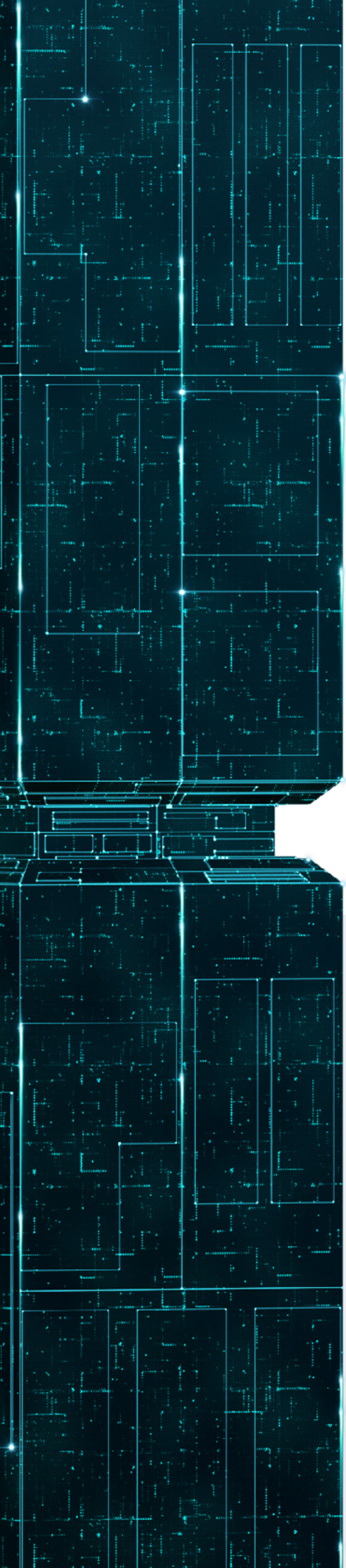
Centralne zarządzanie ESET Secure Authentication odbywa się z poziomu przeglądarki internetowej. Rozwiązanie współpracuje z wszystkimi urządzeniami z systemami iOS i Android oraz obsługuje takie metody uwierzytelniania jak proste w użyciu powiadomienia push, aplikacje mobilne, tokeny sprzętowe, klucze FIDO, a także inne, możliwe do skonfigurowania za pomocą ESA SDK. ESET Secure Authentication nie tylko pomaga chronić dane przedsiębiorstwa, w tym także te zgromadzone w chmurze, ale również spełnić wymagania stawiane przez przepisy prawa, w tym RODO.

ESET CHCE WSPIERAĆ ORGANIZACJE W ZAPEWNIENIU SWOIM DANYM SKUTECZNEJ OCHRONY, SZCZEGÓLNIE W TRAKCIE PANDEMII COVID-19, W ZWIĄZKU Z CZYM STANDARDOWY MIESIĘCZNY OKRES PRÓBNY NA ESET SECURE AUTHENTICATION ZOSTAŁ WYDŁUŻONY DO 90 DNI.

POZNAJ ESET SECURE AUTHENTICATION

Warto także pomyśleć o wdrożeniu pełnego szyfrowania dysku, które stanowi bardzo dobre uzupełnienie dla wieloskładnikowego uwierzytelniania. ESET Full Disk Encrytpion to skuteczne narzędzie, które umożliwia szyfrowanie dysków systemowych, poszczególnych partycji oraz całej powierzchni dysków. Rozwiązanie dodatkowo zwiększa bezpieczeństwo danych oraz można nim zarządzać z poziomu konsol zarządzania ESET – ESET Security Management Center oraz ESET Cloud Administrator.





WIEDZA TO POTĘGA... I BEZPIECZEŃSTWO

W bazie wiedzy MITRE ATT&CK można przeanalizować różne techniki ataków na RDP. Do zawartych w niej zasobów odnosi się wielu badaczy bezpieczeństwa, a sama baza stanowi cenne źródło informacji. W połączeniu z rozwiązaniem klasy EDR może się ona stać bardzo użytecznym narzędziem podczas szczegółowej analizy poszczególnych zagrożeń wymierzonych przeciwko sieci danej organizacji. Produkty pokroju ESET Enterprise Inspector (EEI) pozwalają administratorom zbadać wykryte incydenty, zasięgnąć dalszych informacji na ich temat w bazie ATT&CK oraz ustawić spersonalizowane alarmy dla sieci danej organizacji.

W przypadku zagrożeń związanych z RDP może mieć miejsce sytuacja, kiedy dochodzi jedynie do częściowej detekcji, ale sieć pozostaje niezabezpieczona. Rozwiązania klasy EDR mogą pomóc właśnie w takich sytuacjach, kiedy wystąpienie danego incydentu nie może zostać jednoznacznie potwierdzone. Przykładowo, na skutek ataku z wykorzystaniem BlueKeep dany system może natychmiast ulec awarii. W takiej sytuacji aby wykorzystać podatność w RDP może się okazać konieczny dodatkowy atak na inną podatność (np. we Flashu – z wykorzystaniem plików php), który ujawni odpowiednie adresy w pamięci jądra, dzięki czemu napastnik nie będzie musiał ich zgadywać. To umożliwia przestępcom na bardziej precyzyjne działania, zmniejszając ryzyko awarii systemu. Tego typu powiązane zachowania mogą zostać zidentyfikowane z pomocą spersonalizowanych reguł w ESET Enterprise Inspector, zwracając w razie potrzeby uwagę administratora stosownym alarmem. W zdobyciu dodatkowych informacji na temat potencjalnych zagrożeń dla organizacji oraz słabych punktów w jej zabezpieczeniach mogą pomóc regularne testy penetracyjne oraz identyfikowanie podejrzanych zachowań za pomocą narzędzi SIEM, IPS, IDS.

PODSUMOWANIE

Epidemia COVID-19 zmieniła sposób funkcjonowania przedsiębiorstw i to nie tylko w trakcie jej trwania, ale na stałe. Pracodawcy muszą się dostosować do nowej rzeczywistości, w której pracownicy pracują z domu i to nie tylko teraz, ale także w przyszłości.

Pandemia pokazała nam, że wiele zawodów i działalności dotychczas kojarzonych z pracą na miejscu, w biurze, może być wykonywanych zdalnie. Żeby jednak tak się stało, pracownicy zdalni muszą mieć zapewniony bezpieczny dostęp do firmowych zasobów. ESET oferuje szereg rozwiązań, które mogą w tym pomóc, chroniąc firmę w okresie pracy zdalnej.