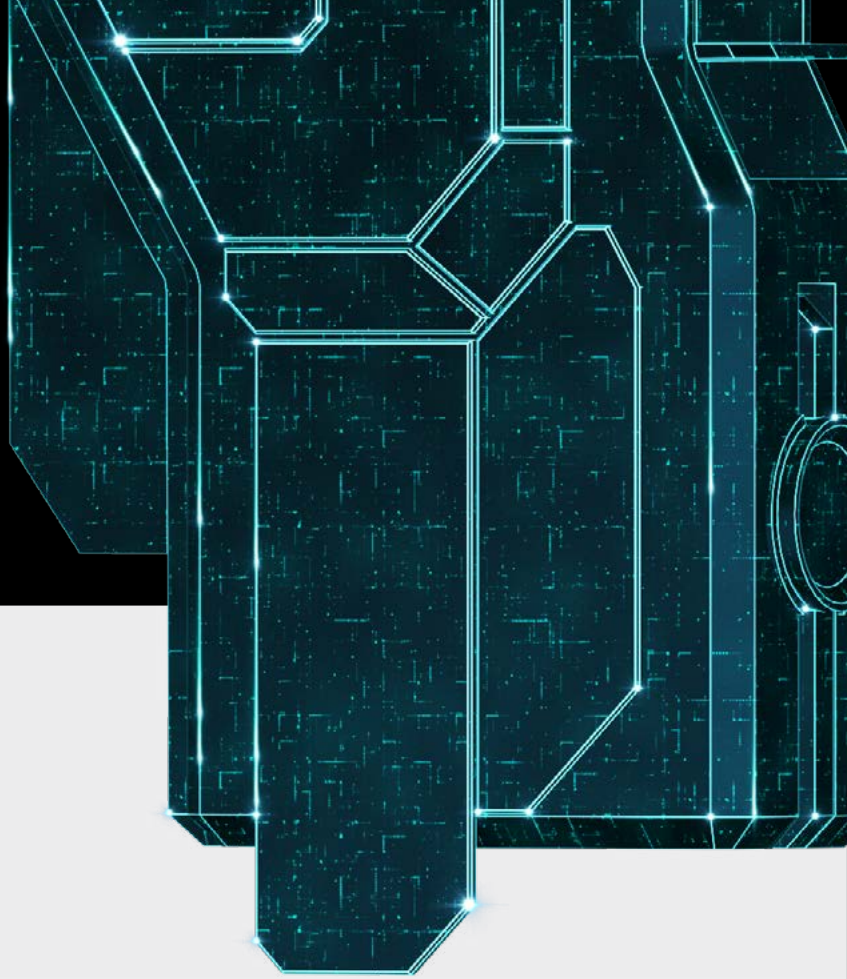


RDP: ZABEZPEČENIE VZDIALENÉHO PRIPOJENIA JE OTÁZKOU DNEŠKA, NIE ĎALEKEJ BUDÚCNOSTI

Využívate na preklenutie súčasnej krízovej situácie vo firemnej sieti možnosť vzdialeného prístupu cez Remote Desktop Protocol (RDP)? V tom prípade by ste mali čo najviac obmedziť hroziace riziká, ktoré sa týkajú práve protokolu pripojenia k vzdialenej ploche. Pomôžu vám osvedčené postupy z praxe, nástroje na overovanie prístupu, ale aj existujúca databáza znalostí.

V dôsledku šíriacej sa pandémie koronavírusu sa množstvo spoločností na celom svete dostalo do situácie, keď museli svojich zamestnancov poslať domov a začať hromadne využívať možnosti práce na diaľku pomocou rôznych dostupných nástrojov. Medzi ne patrí aj technológia RDP, ktorá sa však v uplynulých rokoch viackrát stala terčom kybernetických útokov. Vyskytli sa viaceré prípady narušenia bezpečnosti, hlavne keď sa útočníkom podarilo nájsť spôsob, ako zneužiť zle nakonfigurované nastavenia alebo slabé heslá, a tak získať prístup do firemných sietí.

Keď sa útočníkovi podarí dostať do siete, má voľnú cestu a môže robiť takmer čokoľvek. Výsledkom môže byť napríklad krádež duševného vlastníctva alebo iných citlivých informácií či zašifrovanie zariadenia s cieľom žiadať výkupné.

AUTOR: Aryeh Goretsky
SPOLUPRACOVNÍK: James Shepperd

apríl 2020

1

Ako útočníci zneužívajú RDP?

V posledných rokoch spoločnosť ESET zaznamenala rastúci počet bezpečnostných incidentov, pri ktorých sa útočníci vzdialene pripojili na Windows servery z internetu prostredníctvom RDP a prihlásili sa ako administrátor. Vektory útokov boli v týchto prípadoch rôzne: zraniteľnosti (napr. BlueKeep CVE-2019-0708), phishing, technika známa ako sprejovanie hesiel, útok hrubou silou alebo zle nakonfigurovaný prístup do interných systémov.

Keď sa útočníkom podarí prihlásiť sa na server ako administrátor, zvyčajne najskôr urobia prieskum s cieľom zistiť, na čo server slúži, kto ho používa a v akých časoch. Následne môžu začať so škodlivými úkonmi.

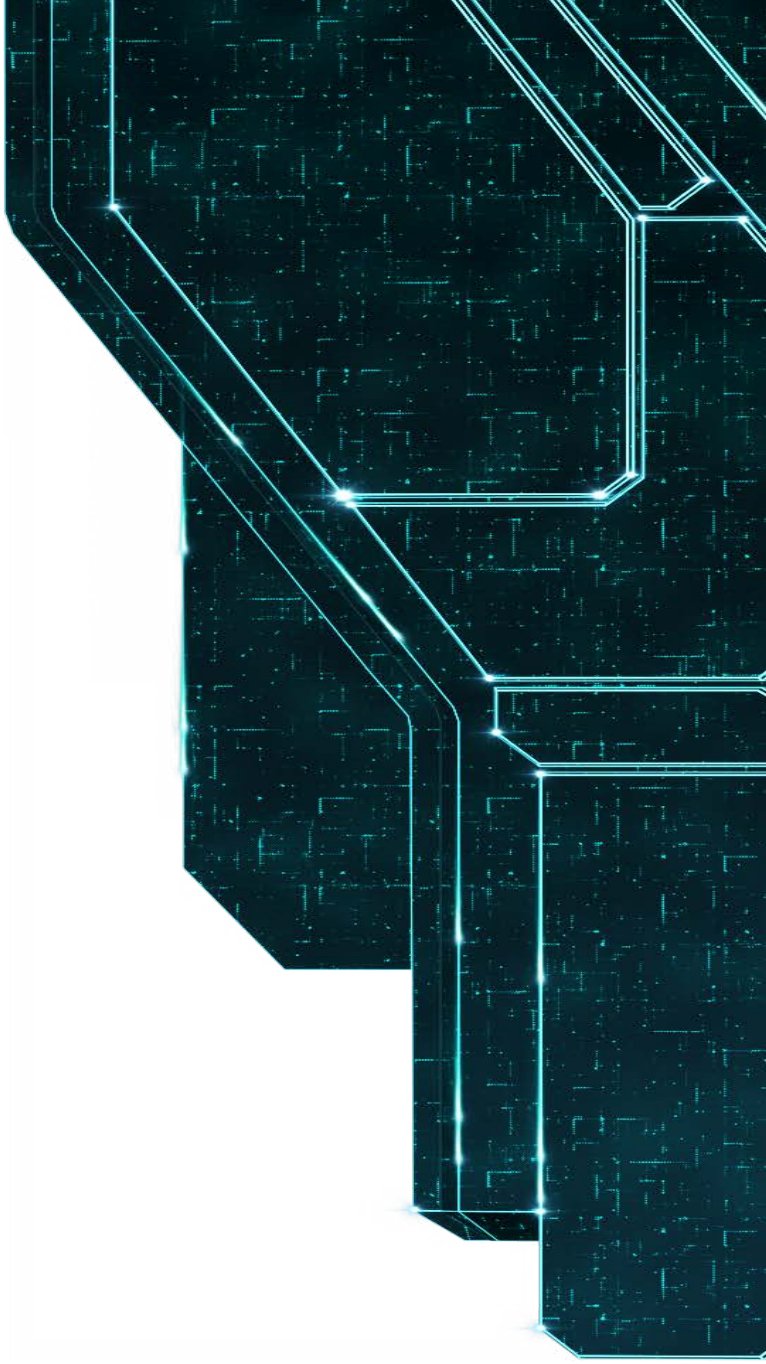
Toto nie je kompletný zoznam možných činností a rovnako nemusí útočník nevyhnutne vykonať všetky z nich. Presná frekvencia, postupnosť a povaha toho, čo útočníci robia, sa od prípadu k prípadu značne líšia.

ČASTÉ ŠKODLIVÉ AKTIVITY, KTORÉ SME ZAZNAMENALI, ZAHŔŇAJÚ:

- vymazanie protokolov obsahujúcich dôkazy o prítomnosti útočníka v systéme,
- vypnutie plánovaných termínov zálohovania a tieňových kópií,
- vypnutie bezpečnostného softvéru alebo nastavenie vylúčení (čo je pre správcov povolené),
- stiahnutie a inštalácia rôznych programov na server,
- vymazanie alebo prepísanie starých záloh, ak sú dostupné,
- exfiltrácia dát zo servera.

TRI NAJBEŽNEJŠIE Z NICH SÚ:

- inštalovanie programov na ťaženie kryptomeny, ako je napr. Monero,
- inštalovanie ransomvéru s cieľom vymáhať peniaze, pričom výkupné sa často platí formou kryptomeny, napr. Bitcoinu,
- v niektorých prípadoch môžu útočníci nainštalovať dodatočný softvér na vzdialené ovládanie, aby si zachovali prístup k napadnutým serverom aj v prípade, že ich aktivita cez RDP bola odhalená a ukončená.



NEDÁVNE PRÍKLADY ŠKODLIVÝCH AKTIVÍT CEZ RDP

GandCrab je názov veľmi produktívneho ransomvéru, ktorý bol aktívny do mája 2019. Autori na jeho ďalšie šírenie použili obchodný model „ransomvér ako služba" (RaaS), v ktorom ponúkaný malvér na svoje vlastné škodlivé aktivity využívalo viacero pridružených kybernetických útočníkov. GandCrab sa zameriaval predovšetkým na poskytovateľov spravovaných služieb (MSP). Použitím RDP sa pripojil na ich nástroje vzdialenej správy a vydieral viacerých zákazníkov súčasne.

Autori ransomvéru GandCrab oznámili ukončenie činnosti po tom, čo FBI zverejnila dešifrovacie kľúče. Naši odborníci sú však toho názoru, že zdrojový kód GandCrab mohol byť predaný inej skupine, ktorá teraz prevádzkuje ransomvér Sodinokibi (naznačujú to zmeny v kóde, jeho štruktúra a nasledujúce aktualizácie). Ransomvér Sodinokibi sa objavil v rovnakom období, ako začal GandCrab ukončovať svoju činnosť. Sodinokibi v podstate vystriedal GandCrab a pri útokoch na poskytovateľov spravovaných služieb (MSP) cez RDP začal používať podobné techniky, stratégiu a postupy ako jeho predchodca.

Zabezpečenie pripojení poskytovateľov spravovaných služieb je mimoriadne dôležité, keďže majú vo svojich rukách „kľúče od vstupnej brány" do tisícok malých a stredných firiem (ako aj ich obchodných partnerov a zákazníkov), no dokonca aj niektorých veľkých organizácií. Pre firmy, ktoré predstavujú klientov MSP, sa využívanie spravovaných služieb stalo nevyhnutnosťou, keďže tímy aj jednotliví používatelia potrebujú od správcov pomoc pri rôznych procesoch, od licencovania a aktualizácií až po samotné zabezpečenie.

ZRANITEĽNOSŤ V RDP OTVÁRA DVERE PRE ÚTOČNÍKOV

Počet útokov cez RDP pomaly, ale isto narastá. Pozornosť im venujú aj mnohé vládne inštitúcie, ako je napríklad americká FBI, centrá kybernetickej bezpečnosti v Spojenom kráľovstve (NCSC), Kanade (CCCS) či Austrálii (ACSC).

Veľké riziko útokov prišlo v máji 2019 s objavením zraniteľnosti CVE-2019-0708, tiež známej pod označením „BlueKeep". Táto bezpečnostná diera v RDP ovplyvňuje systémy Windows 2000, Windows XP, Windows Vista, Windows 7, Windows Server 2003, Windows Server 2003 R2, Windows Server 2008 a Windows Server 2008 R2*.

Hoci ide o staršie operačné systémy, ktoré vo väčšine prípadov už nie sú podporované alebo majú iba obmedzenú podporu výrobcu, telemetrické dáta naznačujú, že mnohé z týchto zraniteľných systémov sa stále používajú.

Zraniteľnosť BlueKeep umožňuje útočníkom na napadnutých zariadeniach spúšťať ľubovoľný kód. S využitím automatizovaných nástrojov môžu aj individuálni útočníci predstavovať rýchlo sa šíriacu hrozbu. Táto zraniteľnosť je však nebezpečná v tom, že útočníci môžu vytvoriť červa, ktorý si túto bezpečnostnú dieru nájde a prostredníctvom nej sa bude automaticky ďalej šíriť v rámci siete aj mimo nej bez toho, že by si vyžadoval akýkoľvek zásah používateľa. Niečo podobné sme mohli v minulosti pozorovať napríklad pri červoch Conficker a Win32/Diskcoder.C (tiež pod označením NotPetya).

SPOLOČNOSŤ ESET PONÚKA BEZPLATNÝ NÁSTROJ NA DETEKCIU ZRANITEĽNOSTI BLUEKEEP (CVE-2019-0708), KTORÝ POMÁHA IDENTIFIKOVAŤ SYSTÉMY OHROZENÉ ZNEUŽITÍM BEZPEČNOSTNÝCH CHÝB V RDP. NA NASLEDUJÚCOM ODKAZE SA DOZVIETE VIAC O DETEKČNOM NÁSTROJI, KTORÝ SI MÔŽETE ZADARMO STIAHNUŤ A VYSKÚŠAŤ.

VIAC O DETEKČNOM NÁSTROJI

**Poznámka:* *Zraniteľnosť BlueKeep podľa informácií dostupných v čase písania tohto textu neovplyvňuje systémy Windows 8, Windows Server 2012 ani novšie verzie.*

Zneužitie zraniteľností, pre ktoré môže byť vytvorený červ, je vo všeobecnosti považované za vážny problém. Spoločnosť Microsoft priradila zraniteľnosti najvyššiu úroveň závažnosti a vo zverejnených pokynoch pre zákazníkov ju označila ako kritickú. V národnej databáze zraniteľností, ktorá patrí pod správu vlády Spojených štátov amerických, je pri zázname CVE-2019-0708 uvedená závažnosť na úrovni 9,8 z 10. Spoločnosť Microsoft tiež uverejnila článok, v ktorom dôrazne odporúča, aby si používatelia nainštalovali bezpečnostné záplaty, pričom vydala záplaty dokonca aj pre nepodporované operačné systémy Windows XP a Windows Server 2003. Obavy zo zneužitia zraniteľnosti boli také veľké, že začiatkom júna 2019 vydala Národná bezpečnostná agentúra Spojených štátov amerických výnimočné odporúčanie na inštaláciu záplat spoločnosti Microsoft súvisiacich s touto bezpečnostnou chybou.

O zraniteľnosti sa veľa hovorilo medzi penetračnými testermi po celom svete, no žiadne významné zvýšenie aktivity spojenej s BlueKeep nebolo zaznamenané až do novembra 2019, keď sa na verejnosť dostali správy o použití exploitu, o čom informovali portály ZDNet a WIRED. Útoky údajne neboli veľmi úspešné, keďže asi na 91 % zraniteľných počítačov došlo k pádu systému s vypísaním chyby a zobrazením modrej obrazovky (BSoD), keď sa útočník pokúsil o zneužitie zraniteľnosti BlueKeep. Na zvyšných 9 % zraniteľných počítačov však útočníci úspešne nainštalovali softvér na ťaženie kryptomeny Monero. Nešlo síce o obávaný útok, pri ktorom by bol použitý samostatne sa šíriaci červ, no skupine kybernetických zločincov sa v tomto prípade podarilo zautomatizovať zneužitie zraniteľnosti, i keď len s nízkou mierou úspešnosti.

Keďže čas hrá v takýchto situáciách dôležitú úlohu, namiesto príliš podrobného popisu zraniteľnosti sa zameriame skôr na to, aké kroky podniknúť na zabezpečenie siete pred touto hrozbou.

2.

Ochrana pred útočníkmi zneužívajúcimi RDP

Ako sa teda chrániť? Prvým krokom je prestať využívať RDP na priame pripájanie na firemné servery prostredníctvom internetu, prípadne takéto použitie RDP aspoň čo najviac obmedziť. Toto môže byť dnes pre mnohé podniky obzvlášť problematické, keďže veľká časť zamestnancov pracuje na diaľku v rôznych karanténnych režimoch.

V prípade, že v sieti stále máte počítače so systémom Windows Server 2008 alebo Windows 7 (verzie, ktoré od januára 2020 už nie sú podporované), ku ktorým je možné sa priamo pripájať cez RDP, je vaša firma vystavená vážnej hrozbe možného útoku a odporúčame vám preto bezodkladne prijať potrebné opatrenia na zmiernenie rizika. Používaním nepodporovaných verzií operačného systému sa veľmi výrazne rozširuje škála možných útokov. Nasledujúce odporúčania by preto mali prísť na rad až po aktualizovaní systémov na novšie verzie, pre ktoré ich výrobcovia poskytujú plnú podporu.

Ak vo firme používate aktuálne verzie operačného systému, nie je nutné okamžite prestať s používaním RDP, no takéto vzdialené pripájanie by ste mali čo najskôr a čo najdôkladnejšie zabezpečiť. S týmto cieľom sme vytvorili tabuľku, ktorá obsahuje 12 odporúčaných krokov, ktoré vám môžu pomôcť lepšie zabezpečiť počítače pred útokmi zneužívajúcimi RDP.

12 ODPORÚČANÍ, AKO ZABEZPEČIŤ RDP

Poradie v tejto tabuľke je voľne založené na dôležitosti a jednoduchosti zavádzania jednotlivých krokov, no v konečnom dôsledku bude vždy závisieť od konkrétnej firmy. Niektoré odporúčania sa na vašu firmu napríklad nemusia vzťahovať alebo môže byť praktickejšie ich zavádzať v inom poradí. Rovnako možno bude potrebné podniknúť aj nejaké dodatočné kroky.

	ODPORÚČANIE	ZDÔVODNENIE
1	Zakážte externé pripojenia k lokálnym počítačom na porte 3389 (TCP/UDP) vo firewalle na okraji siete.*	Úplne sa zablokuje prístup cez RDP z internetu.
2	Čo najskôr otestujte a nasaďte záplaty na zraniteľnosť CVE-2019-0708 (BlueKeep) a povoľte overovanie na úrovni siete.	Nainštalovanie záplat od spoločnosti Microsoft a ďalší postup podľa jej pokynov pomáha zabezpečiť ochranu zariadení pred zraniteľnosťou BlueKeep.
3	Všetky účty, do ktorých je možné sa prihlásiť cez RDP, by mali využívať komplexné heslá (povinná by mala byť dlhá prístupová fráza obsahujúca 15 a viac znakov bez slovných spojení, ktoré sa týkajú firmy, názvov produktov alebo používateľov).	Týmto je možné predísť útokom cieleným na uhádnutie správnych hesiel a útokom známym ako „credential stuffing“, čo je masívne testovanie už uniknutých prihlasovacích údajov. Tieto techniky je veľmi jednoduché zautomatizovať. Navýšenie počtu znakov v heslách exponenciálne zvyšuje ich odolnosť voči útokom.
4	Pri prístupe k serverom cez lokálne účty s právami správcu by sa mali používať jedinečné heslá (napr. s využitím nástroja LAPS alebo účinnej služby na správu hesiel). * *Zároveň odporúčame, aby prístupové práva k serverom mala iba obmedzená skupina používateľov.*	*(ako je uvedené vyššie)* Obmedzením počtu používateľov s povoleným prístupom sa zredukujú aj možné miesta útokov na dané servery.
5	Ak je to možné, pre pripojenia klienta RDP nastavte „vysokú“ úroveň šifrovania. V opačnom prípade použite pre pripojenia čo najvyššiu dostupnú úroveň šifrovania.	Ak je to možné, použite 128-bitové šifrovanie pre všetku komunikáciu medzi klientom a serverom.

6	Nainštalujte riešenie viacúrovňového overovania (MFA), ako je napríklad ESET Secure Authentication (ESA), a vynúťte jeho používanie pre všetky účty, do ktorých je možné sa prihlasovať cez RDP, ako aj pre všetky účty správcu.	Pri prihlasovaní do počítačov sa bude vyžadovať aj druhá úroveň overenia, ktorá je dostupná výhradne pre zamestnancov prostredníctvom mobilného telefónu, tokenu alebo iného mechanizmu.
7	Nainštalujte bránu virtuálnej súkromnej siete (VPN) na sprostredkovanie všetkých externých pripojení cez RDP, ktoré neprichádzajú z vašej lokálnej siete.	Zabráni sa tak priamym pripojeniam cez RDP medzi internetom a lokálnou sieťou. Zároveň vám tento krok umožní vynútiť prísnejšie požiadavky na identifikáciu a autentifikáciu pri vzdialenom prístupe k počítačom.
8	Prostredníctvom riadiaceho panela sa uistite, že váš bezpečnostný softvér pre koncové zariadenia je chránený heslom, ktoré je dostatočne silné a neviaže sa so správcovskými a servisnými účtami. ESET Security Management Center (ESMC) umožňuje jednoduchú, no podrobnú kontrolu založenú na politikách, ako aj vytváranie rôznych skupín počítačov. Zároveň je ESMC multitenantné a umožňuje prihlasovanie chrániť viacúrovňovým overovaním (MFA).	Týmto sa zabezpečí dodatočná vrstva ochrany pre prípad, že by útočník získal prístup do siete.
9	Zapnite blokovanie zneužití v bezpečnostnom softvéri na koncových zariadeniach. Ide o technológiu určenú na detekciu anomálií, ktorá monitoruje správanie často zneužívaných aplikácií.	Mnohé bezpečnostné programy pre koncové zariadenia zahŕňajú možnosť blokovať techniky zneužitia zraniteľností. Uistite sa, že táto funkcia je zapnutá.
10	Izolujte od siete akýkoľvek nezabezpečený počítač, ktorý musí byť prístupný z internetu prostredníctvom RDP.	Využite možnosť izolácie od siete, aby ste oddelili zraniteľné počítače od zvyšku siete.
11	Vymeňte nezabezpečené počítače.	V prípade, že počítač nie je možné zabezpečiť pred zraniteľnosťou BlueKeep, naplánujte jeho včasnú výmenu.
12	Zvážte na bráne VPN zaviesť blokovanie na základe GeoIP.	V prípade, že vaši zamestnanci a dodávatelia pôsobia v rovnakej krajine alebo v niekoľkých vybraných krajinách, zvážte možnosť blokovať prístup z vylúčených krajín. Takto zablokujete pripojenia útočníkov z cudziny.

***RDP predvolene používa port 3389**. *Ak ste zmenili predvolený port na inú hodnotu, bude potrebné zablokovať toto zmenené číslo portu.*

3.

Ako ESET pomáha chrániť vaše RDP

V prvom kroku je dobré sa uistiť, že váš bezpečnostný softvér na koncových zariadeniach je aktualizovaný a tiež že deteguje zraniteľnosť BlueKeep. Následne nastupuje komplexnejšia úloha pre viacvrstvovú technológiu. Zraniteľnosť BlueKeep je detegovaná ako RDP/Exploit.CVE-2019-0708 prostredníctvom modulu Ochrany pred sieťovými útokmi. Tento modul je rozšírením technológie firewallu spoločnosti ESET a je súčasťou bezpečnostných produktov ESET na správu koncových zariadení. Endpoint.

Ďalšou kľúčovou vrstvou pre ochranu RDP je technológia ESET Exploit Blocker, ktorá monitoruje často zneužívané aplikácie (webové prehliadače, softvér na zobrazovanie dokumentov, e-mailové klienty, Flash, Java a pod.). Namiesto zameriavania sa na konkrétne identifikátory CVE sleduje techniky zneužití. Každá takto zistená hrozba je na zariadení okamžite zablokovaná.

Popri využívaní ochranných technológií vám odporúčame zaviesť vhodné procesy a nástroje, ktoré by mali byť čo najjednoduchšie z pohľadu použiteľnosti. Na zabezpečenie RDP je potrebných viacero procesných úkonov a krokov, no azda najdôležitejšiu úlohu môže zohrať ľahko použiteľné viacúrovňové overovanie (MFA). Vďaka takémuto riešeniu vo firme predídete používaniu hesiel, ktoré je možné ľahko uhádnuť alebo prelomiť technikou hrubej sily. Keď sa zameriate na overovanie prístupu do systému alebo platformy, v tomto prípade RDP, zaistíte si kľúčovú vrstvu ochrany pre celú sieť aj jednotlivých používateľov.

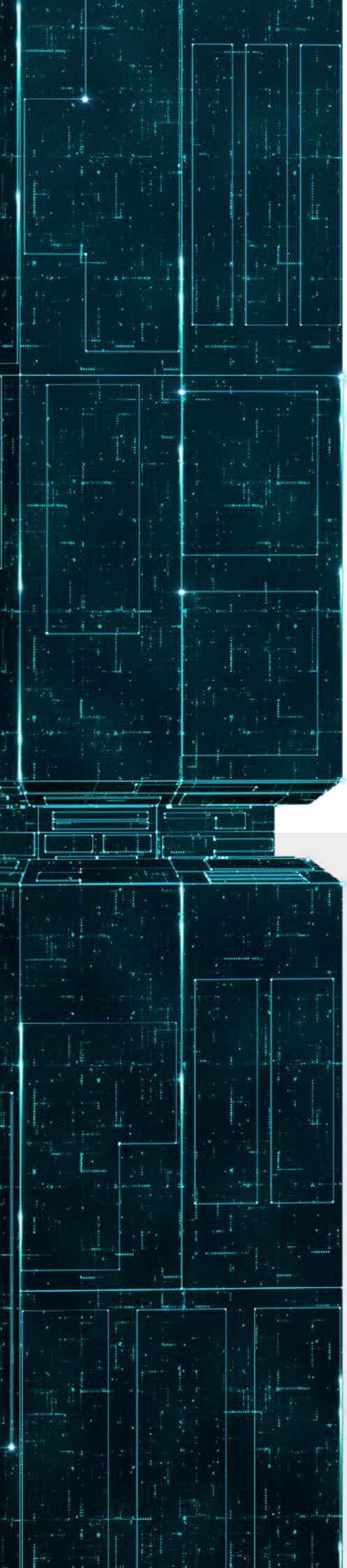
Naše riešenie ESET Secure Authentication (ESA) pomocou viacúrovňového overovania pomáha chrániť rôzne druhy zraniteľnej komunikácie, akou je aj pripájanie k vzdialenej ploche cez RDP.

Riešenie ako ESA podporuje všetky siete VPN (čo je tiež dôležitá vrstva zabezpečenia prístupu) a umožňuje zabezpečiť prihlasovanie do kritických zariadení, ktoré obsahujú citlivé údaje, ako aj do cloudových služieb Office 365, Google Apps či Dropbox, prípadne mnohých iných služieb používajúcich ADFS 3.0 alebo SAML.

Riešenie ESA sa spravuje centrálne z prehliadača a je možné ho používať na všetkých zariadeniach iPhone aj Android, pričom tiež podporuje viacero spôsobov overenia vrátane ľahko ovládateľných push notifikácií, mobilných aplikácií, hardvérových tokenov, bezpečnostných kľúčov FIDO a iných vlastných metód (prostredníctvom ESA SDK). ESA pomáha chrániť firemné dáta a cloud jednoduchým a pritom účinným spôsobom.

PREHĽAD RIEŠENIA ESET SECURE AUTHENICATION

Ďalším vhodným krokom po zavedení MFA je aj pridanie šifrovania disku. ESET Full Disk Encryption (EFDE) poskytuje výkonné šifrovanie systémových diskov, jednotlivých oblastí alebo celých diskov. Šifrovanie je spravované natívnymi konzolami určenými na vzdialenú správu – ESET Security Management Center a ESET PROTECT Cloud. Týmto spôsobom je možné výrazne posilniť zabezpečenie firemných dát.



V ZNALOSTIACH JE SILA, V PLNOM ZABEZPEČENÍ VŠAK TIEŽ

Možnosť prečítať si podrobné informácie o rôznych technikách a stratégiách útokov cez RDP ponúka databáza znalostí na platforme MITRE ATT&CK. Využívajú a odvolávajú sa na ňu výskumní pracovníci viacerých výrobcov bezpečnostných riešení, no platforma je zdieľaným zdrojom informácií. Platforma ATT&CK a súvisiace nástroje EDR (Endpoint Detection and Response) môžu byť veľmi užitočné pri detailnom skúmaní hrozieb, ktorým vaša sieť čelí. Nástroje ako ESET Enterprise Inspector (EEI) umožňujú bezpečnostným správcom preskúmať detekcie, priamo získať doplňujúce informácie o hrozbe či útoku zo znalostnej databázy ATT&CK, ako aj nastaviť vlastné výstražné upozornenia v rámci siete.

V prípade hrozieb využívajúcich RDP však niekedy môže dochádzať len k čiastočným detekciám, a tak nie je zaručená úplná ochrana. Nástroje EDR môžu byť užitočné práve aj v takých situáciách, keď nedochádza k jednoznačným detekciám. V niektorých prípadoch napríklad exploit BlueKeep okamžite spôsobil pád cieľového systému, pretože sa ukázal ako nespoľahlivý. Exploit, ktorý zneužíva zraniteľnosť v RDP, môže na svoje fungovanie potrebovať spárovanie s exploitom inej zraniteľnosti, napríklad vedúcej k odhaleniu informácií (napr. prostredníctvom Flash – PHP súborov). Zneužitím takejto zraniteľnosti sa odkryjú adresy pamäte jadra a už nie je potrebné ich hádať. Exploit potom pomocou techniky zvanej „heap spraying" umiestni kód všade na potrebné miesto v pamäti, čím sa zníži pravdepodobnosť pádu systému pri následnom útoku. Na základe vlastných pravidiel vytvorených v EEI môže byť takéto pridružené správanie označené príznakom a zároveň môže vyvolať aj výstražné upozornenie pre správcu. Podrobné informácie o sieti je možné získavať aj prostredníctvom pravidelného penetračného testovania a monitorovania podozrivého správania pomocou nástrojov SIEM, IPS a IDS.

ZÁVER

Pandémia ochorenia COVID-19 zmenila spôsob, akým firmy pracujú, a to nie iba dočasne, ale zrejme už natrvalo. Zamestnávatelia sa musia prispôsobovať požiadavkám zamestnancov pracujúcich z domu už dnes, ale rovnako to bude platiť aj v budúcnosti.

Pandémia nám ukázala, že mnohé profesie a úlohy, pri ktorých sa prítomnosť zamestnancov na pracovisku predtým považovala za nevyhnutnú, sa budú prehodnocovať z hľadiska možného výkonu práce na diaľku. Takáto zmena si však vyžaduje, aby bol vzdialený prístup zamestnancov do firmy dobre zabezpečený. Spoločnosť ESET ponúka celú škálu riešení, ktoré pomáhajú firmám a organizáciám zaistiť bezpečný prístup k ich digitálnym zdrojom.