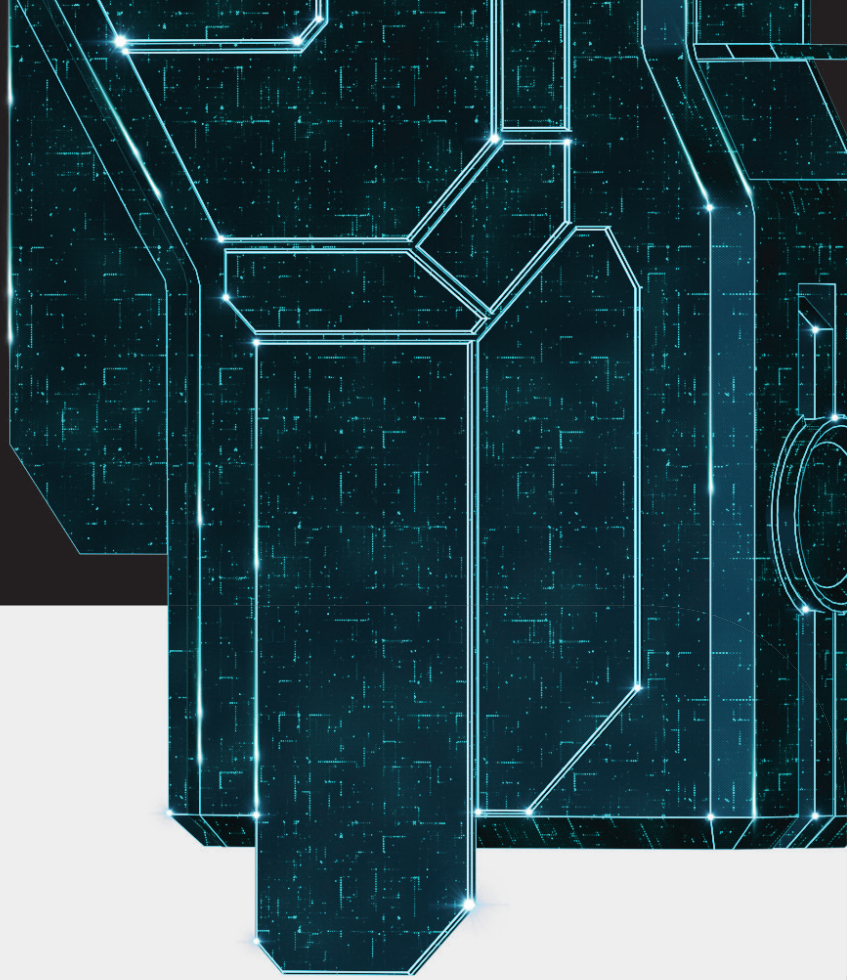
CYBERSECURITY
EXPERTS ON YOUR SIDE



RDP: CONFIGURAREA SECURITĂȚII PENTRU UN VIITOR REMOTE, NU FOARTE ÎNDEPĂRTAT

Vă sprijiniți pe protocolul Remote Desktop (RDP) pentru a vă administra rețeaua în timpul unei situații excepționale? În acest caz asigurați-vă că limitați potențialele riscuri cu ajutorul unor bune practici, folosind instrumente de autentificare și apelând la baza de cunoștințe existentă.

Pandemia COVID-19 a forțat companiile de pretutindeni să-și treacă angajații pe un sistem de lucru de acasă și să implementeze la nivel de infrastructură business un mod de lucru remote, de la distanță, folosind orice mijloace disponibile. Printre ele se numără și tehnologia RDP, care a fost, însă, ținta multor atacuri cibernetice specifice în ultimii ani. Incidentele de securitate au apărut mai ales atunci când atacatorii au identificat modalități de a exploata setările configurate necorespunzător sau parolele slabe pentru a avea acces la rețelele companiei.

Odată pătrunși în interior, atacatorii au găsit drum liber pentru a realiza aproape orice acțiune dorită, inclusiv subtilizarea proprietăților intelectuale sau a altor informații sensibile, putând chiar să opteze pentru criptarea datelor stocate în infrastructura compromisă, ca să ceară o răscumpărare în schimbul recâștigării accesului la ele.

AUTOR:Aryeh Goretsky
CORESPONDENT: James Shepperd

Aprilie 2020

1.

Ce atacuri vizează RDP?

În ultimii ani, ESET a înregistrat un număr tot mai mare de incidente în care atacatorii s-au conectat de pe internet, de la distanță, la serverele Windows folosind RDP și s-au autentificat în cele din urmă ca administratori de sistem. Aceaste breșe au implicat mulți vectori prin care atacurile au fost derulate: vulnerabilități (cum ar fi BlueKeep CVE-2019-0708), mesaje de tip phishing, credential stuffing, password spraying, forță brută sau acces configurat necorespunzător către sistemele interne.

Odată ce atacatorii se conectează la un server cu drepturi de administrare, într-o primă fază ei vor menține discreția, într-o misiune de recunoaștere a scopului acelui server, de către cine este utilizat și când este folosit. Apoi vor începe să efectueze acțiunile rău intenționate pe care le vizează.

Veți găsi mai jos o listă cu principalele acțiuni malițioase pe care le pot derula atacatorii, însă este puțin probabil că vor reuși să ducă la bun sfârșit toate aceste activități. Frecvența, ordinea acțiunilor și natura a ceea ce vor face atacatorii, după ce reușesc să se infiltreze, variază în funcție de mulți factori.

PRINTRE ACTIVITĂȚILE MALIȚIOASE COMUNE PE CARE LE-AM IDENTIFICAT SE NUMĂRĂ:

- ștergerea fișierelor de log care conțin dovezi ale prezenței lor în sistem
- dezactivarea back-up-urilor programate și a copiilor shadow
- dezactivarea software-ului de securitate sau configurarea unor reguli de excludere (drept de care beneficiază doar administratorii)
- descărcarea și instalarea unor diverselor programe pe server
- ștergerea sau suprascrierea unor copii de rezervă vechi, dacă sunt accesibile
- sustragerea datelor de pe server

TREI DINTRE CELE MAI FRECVENTE ACȚIUNI:

- instalarea programelor de coin-mining pentru a genera criptomonede, de pildă Monero
- instalarea ransomware-ului pentru a extorca organizația, adesea cerând ca răscumpărarea să fie plătită în criptocurrency (bitcoin)
- în unele cazuri, atacatorii ar putea instala software suplimentar de control de la distanță pentru a menține accesul la serverele compromise în cazul în care activitățile lor RDP sunt descoperite și contracarate într-o primă fază

ACTIVITĂȚI MALIȚIOASE RECENTE CARE AU IMPLICAT RDP

Un atac ransomware de amploare, numit de specialiști, GandCrab, a funcționat până în mai 2019 și a folosit un model de business Ransomware-as-a-Service (RaaS) în care dezvoltatorii lui au utilizat serviciile unor alți infractori cibernetici afiliați pentru a distribui mai departe conținut malware. GandCrab, a vizat în special MSP-urile care folosesc RDP pentru a se conecta la instrumentele lor de administrare de la distanță și pentru a extorca simultan clienții care aparțineau acestora.

Deși operatorii de ransomware GandCrab și-au anunțat retragerea după ce FBI a lansat cheile pentru decriptarea ransomware-ului, experții noștri consideră că dezvoltatorii GandCrab au vândut codul sursă către un alt grup care rulează Sodinokibi, (din cauza modificărilor codului, structurii sale și actualizărilor derulate ulterior). Ransomware-ul Sodinokibi a apărut în momentul în care GandCrab a anunțat **suspendarea** operațiunilor, folosind tactici, tehnici și proceduri similare cu ale predecesorului său pentru a viza MSP-urile prin RDP.

Atracția către MSP este notabilă și poate fi ușor de anticipat, întrucât MSP-urile dețin, putem spune, 'cheile regatului' având conexiune cu mii de IMM-uri (și cu relațiile de afaceri ale acestor IMM-uri). Din punctul de vedere al clientului MSP, companiile se confruntă cu dependențe similare, atât echipele cât și utilizatorii individuali depinzând în acest sistem de admini pentru servicii de suport complete, de la licențiere și până la actualizări la securitate.

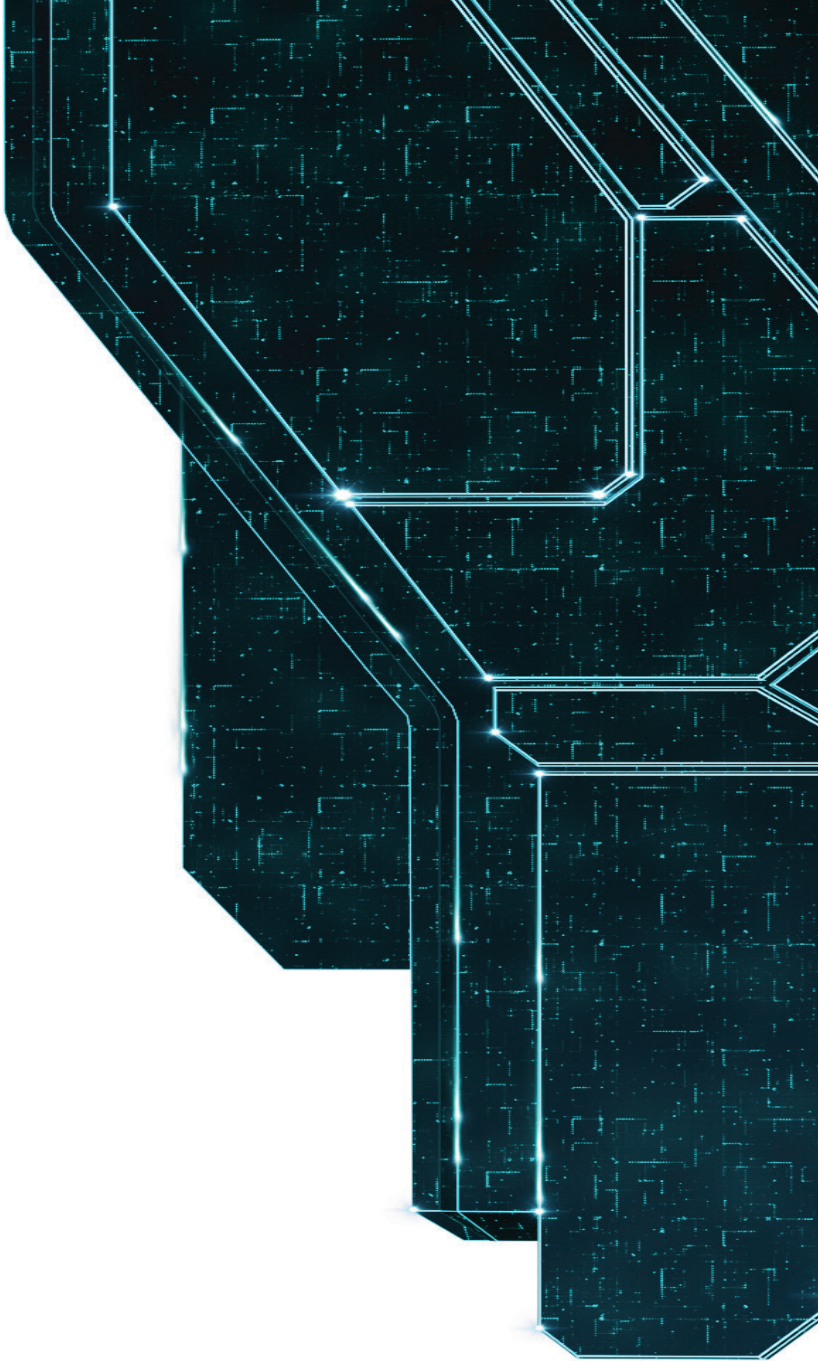
VULNERABILITĂȚILE RDP DESCHID CALEA CĂTRE MAI MULTE RISCURI

Atacurile prin intermediul RDP au început ușor, dar constant, să cunoască o pantă ascendentă, motiv pentr care au fost luate în vizorul mai multor notificări guvernamentale emise de către FBI, NCSC - din Regatul Unit, CCCS, - din Canada și ACSC – din Australia, pentru a aminti doar o parte dintre autoritățile care s-au concentrat asupra lor.

În mai 2019, am asistat la o problemă majoră de securitate odată cu apariția CVE-2019-0708, numită „BlueKeep", o vulnerabilitate a securității în RDP care afectează Windows 2000, Windows XP, Windows Vista, Windows 7, Windows Server 2003, Windows Server 2003 R2, Windows Server 2008 și Windows Server 2008 R2 *

Deși acestea pot fi considerate sisteme vechi și, în majoritatea cazurilor, nu mai sunt acceptate pentru suport sau au doar asistență limitată la nivelul vânzărilor, telemetria sugerează că vor coexista în continuare multe astfel de sisteme vulnerabile.

Vulnerabilitatea BlueKeep permite atacatorilor să ruleze un cod arbitrar pe computerele victimelor lor. Chiar și atacatorii individuali pot răspândi amenințarea folosind instrumente automate pentru atacuri, această vulnerabilitate fiind considerată „wormable", ceea ce înseamnă că un atac s-ar putea răspândi automat în rețele fără nicio intervenție a utilizatorilor, la fel ca Win32 / Diskcoder.C (aka NotPetya) și viermii Conficker din trecut.



ESET OFERĂ UN INSTRUMENT GRATUIT DE DETECTARE BLUEKEEP (CVE- 2019-0708) PENTRU A AJUTA LA IDENTIFICAREA SISTEMELOR VULNERABILE ÎN FAȚA EXPLOATĂRII PRIN RDP. PENTRU INSTRUCȚIUNI PRIVIND UTILIZAREA LUI ȘI PENTRU A DESCĂRCA O COPIE

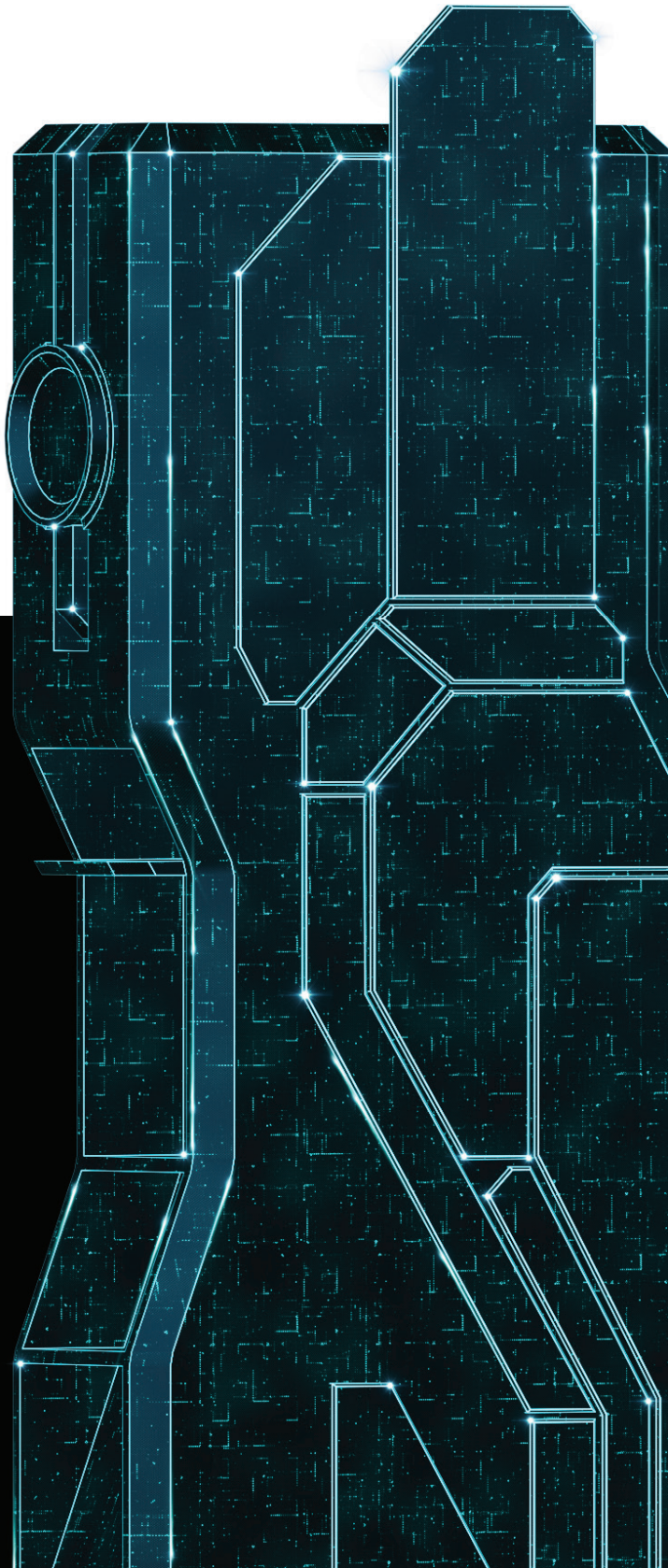
PARCURGEȚI ACEST ARTICOL

**Vă rugăm să rețineți:* versiunile Windows 8 și Windows Server 2012 sau cele mai noi sunt raportate ca fiind neafectate la momentul publicării acestei prezentări.*

Exploatarea vulnerabilităților wormable este, în general, considerată o problemă severă. Microsoft a atribuit vulnerabilității cel mai înalt nivel de severitate, Critical, în ghidul publicat pentru clienți și în baza de date națională pentru vulnerabilități a guvernului american, pericolul reprezentat de CVE-2019-0708 fiind notat cu 9,8 din 10. Microsoft a emis o postare pe blog prin care recomandă urgent și ferm utilizatorilor să-și instaleze patch-urile puse la dispoziție, inclusiv cele pentru sistemele de operare care nu mai beneficiază de suport, cum ar fi Windows XP și Windows Server 2003. Preocupările cu privire la această exploatare de tip wormable au fost atât de mari încât, la începutul lunii iunie 2019, Agenția Națională de Securitate a SUA a emis un document ce conține o serie de sfaturi prin care se recomandă instalarea de patch-uri Microsoft pentru acea amenințare.

Până în noiembrie 2019 nu s-au raportat escaladări majore ale activității BlueKeep, când rapoartele utilizării în masă ale exploatării au devenit publice, după cum au notat ZDNet și WIRED. Se pare că atacurile au fost mai puțin reușite, aproximativ 91% dintre computerele vulnerabile s-au confruntat doar cu o eroare de închidere (ecranul albastru) atunci când atacatorul încerca să exploateze vulnerabilitatea BlueKeep. Cu toate acestea, pe restul de 9% din computerele vulnerabile, acești atacatori au instalat cu succes software-ul Monero crypto-mining. Deși nu este un atac wormable de temut, grupul infracțional a automatizat exploatarea, însă fără o rată mare de succes.

Întrucât timpul este esențial, vom evita o descriere detaliată a acestor vulnerabilități și, în schimb, ne vom concentra asupra a ceea ce ar trebui făcut pentru a proteja rețelele împotriva acestui tip de risc.



2.

Apărarea împotriva atacatorilor RDP

Ce puteți face? Primul lucru este să renunțați la a vă conecta direct la serverele dvs. prin internet când folosiți RDP sau cel puțin să minimizați acest lucru ori de câte ori este posibil. Acest lucru poate fi problematic pentru multe companii, mai ales acum că mulți angajați lucrează de la distanță, pe fondul crizei provocate de COVID-19.

Dacă încă rulați Windows Server 2008 sau Windows 7 (care nu mai beneficiază de suport din ianuarie 2020) și aveți mașini care utilizează aceste platforme care sunt accesibile direct prin RDP, vă supuneți unui risc ridicat de atac și ar trebui să implementați imediat soluțiile de remediere oferite. Prin rularea acestor platforme, șansele dvs. de a fi atacați au crescut considerabil, iar **recomandările de mai jos ar trebui să fie un motiv suplimentar pentru care platformele dvs. de business ar trebui actualizate la cea mai nouă versiune oferită de furnizori.**

Pentru cei care rulează platforme actualizate, situația nu impune oprirea imediată a utilizării RDP, ci adoptarea unor măsuri suplimentare pentru a-l securiza cât mai curând și în detaliu. Pentru a veni în întâmpinarea problemelor dvs., am creat un tabel cu **12 pași pe care îi puteți parcurge pentru a verifica securizarea computerelor dvs. împotriva atacurilor bazate pe RDP.**

12 RECOMANDĂRI PENTRU SECURIZAREA RDP

Acest tabel se bazează pe ordinea importanței și ușurinței implementării, dar poate varia în funcție de organizația dvs. Unele sfaturi pot să nu fie aplicabile sau pot fi mai practice de efectuat într-o ordine diferită. De asemenea, este posibil ca organizația dvs. să aibă nevoie de măsuri suplimentare.

	RECOMANDĂRI	MOTIV
1	Nu permiteți conexiuni externe pe mașinile locale pe portul 3389 (TCP / UDP) la firewall-ul perimetru*	Blochează accesul RDP dinspre internet.
2	Testați și implementați patch-uri pentru vulnerabilitatea CVE-2019-0708 (BlueKeep) și activați autentificarea la nivel de rețea cât mai rapid.	Instalarea patch-ului Microsoft și respectarea îndrumărilor cu strictețe ajută la asigurarea protejării dispozitivelor împotriva vulnerabilității BlueKeep.
3	Pentru toate conturile care pot fi conectate prin RDP, solicitați parole complexe (este obligatorie implementarea unei parole lungi care conține peste 15 caractere, fără referințe la numele companiei, nume de produse sau utilizatori).	Protejează împotriva atacurilor de tip *password-guessing* și *credential-stuffing*. Este foarte de ușor de automatizat și creșterea complexității parolelor le face exponențial mai rezistente la atacuri.
4	Pentru a accesa serverele, utilizați parole unice pentru conturile locale cu drepturi de administrare (de exemplu, folosind LAPS sau un serviciu robust de gestionare a parolelor) **De asemenea: Limitați drepturile de acces la un grup*	*(ca mai sus)* Reduce suprafața de atac a serverelor prin limitarea numărului de utilizatori care le pot accesa.
5	Setați, dacă este posibil, nivelul de criptare al conexiunii clientului RDP la "high". Dacă nu, utilizați cel mai înalt nivel de criptare disponibil pentru conexiuni.	Utilizați criptarea pe 128 de biți pentru toate comunicațiile client-server, dacă este posibil.

6	Instalați o soluție de autentificare multi-factor (MFA), cum ar fi ESET Secure Authentication (ESA), și solicitați implementarea acesteia pentru toate conturile care pot fi conectate prin RDP, precum și pentru toate conturile de administrator.	Necesită un al doilea nivel de autentificare, disponibilă doar pentru angajați printr-o aplicație dedicată de pe smartphone, un token sau prin alt mecanism de autentificare.
7	Instalați un gateway VPN (virtual private network) pentru a media toate conexiunile RDP din afara rețelei dvs. locale.	Împiedică realizarea conexiunilor RDP între internet și rețeaua dvs. locală. Vă permite să impuneți cerințe mai puternice de identificare și autentificare pentru accesul de la distanță la computere.
8	Prin intermediul mediului general de gestionare a securității, asigurați-vă că software-ul dvs. de securitate endpoint este protejat cu o parolă complexă. ESET Security Management Center (ESMC) permite controlul ușor și granular al politicilor și crearea diferitelor grupuri de calculatoare. Simultan, ESMC dispune de o arhitectură multitenancy și se poate accesa prin autentificare MFA.	Oferă un nivel suplimentar de protecție în cazul în care un atacator preia accesul asupra unui cont cu drepturi administrator la rețeaua dvs.
9	Activați funcția blocare a exploit-urilor în software-ul de securitate endpoint utilizat, care este o tehnologie de detectare a anomaliilor care nu se bazează pe semnături, ce monitorizează comportamentul aplicațiilor vizate cel mai des în acest tip de atacuri.	Multe soluții de securitate endpoint pot bloca tehnicile de exploatare. Verificați dacă această funcționalitate este activată în produsul folosit.
10	Izolați orice computer nesigur care trebuie accesat de pe internet folosind RDP.	Implementați izolarea rețelei pentru a bloca computerul (computerele) vulnerabile de restul rețelei.
11	Înlocuiți computerele nesigure.	Dacă un computer nu poate fi actualizat (împotriva vulnerabilității BlueKeep), propuneți înlocuirea sa în timp util.
12	Luați în considerare instituirea blocării în funcție de GeoIP la nivel de gateway VPN.	Dacă personalul și furnizorii se află în aceeași țară sau într-o listă scurtă de țări, luați în considerare blocarea accesului din țările excluse pentru a preveni conexiunile atacatorilor străini.

*RDP operează în mod implicit pe portul 3389. *Dacă ați modificat valoarea acestui port, atunci tot acela trebuie blocat, dar conform valorii pe care ați atribuit-o.*

3.

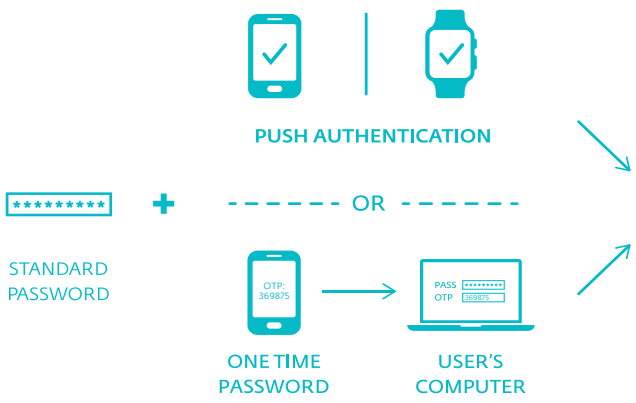
Cum vă ajută ESET să protejați conexiunile RDP

Un prim bun pas este să vă asigurați că software-ul dvs. de securitate endpoint este actualizat și detectează vulnerabilitatea BlueKeep. Merită îndreptată apoi atenția către un rol mai granular pentru tehnologia stratificată de protecție. BlueKeep este detectat drept RDP / Exploit.CVE- 2019- 0708 de către modulul de protecție împotriva atacului la nivel de rețea al ESET, care este o extensie a tehnologiei firewall ESET prezentă în produsele endpoint ESET, începând cu versiunea 7.

Un alt strat de tehnologie esențial pentru protejarea RDP este ESET Exploit Blocker, care monitorizează aplicațiile exploatabile în mod frecvent (browsere, cititoare de documente, clienți de e-mail, Flash, Java și multe altele). Când funcționalitatea detectează ceva, amenințarea este blocată imediat pe mașină respectivă.

În paralel cu tehnologia, vă sfătuim să puneți în aplicare procese adecvate care să fie cât mai ușor de utilizat, procese care în final să beneficiază și ele de pe urma unor instrumente ușor de utilizat. Întrucât securizarea RDP necesită mai multe etape procedurale, autentificarea cu mai mulți factori (MFA) este probabil cea mai importantă, deoarece acționează ca o protecție împotriva parolelor ușor de ghicit sau care pot fi ținta unor atacuri de forța brută. Concentrându-vă pe implementarea unei metode de autentificare pe un sistem sau o platformă, în acest caz RDP, vă protejați unul dintre cele mai critice sisteme pe care le aveți în afacerea dvs. pentru gestionarea securității atât a rețelei dvs. cât și a utilizatorilor individuali.

Soluția noastră MFA, ESET Secure Authentication (ESA) protejează comunicările vulnerabile, cum ar fi Remote Desktop Protocol prin introducerea autentificării cu mai mulți factori.



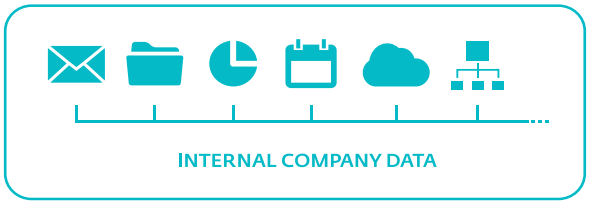
O soluție precum ESA acceptă în toate VPN-urile (care reprezintă în sine o metodă de securizare a accesului), autentificările pe dispozitive critice care conțin date sensibile și servicii cloud precum Office 365, Google Apps sau Dropbox și multe altele care utilizează ADFS 3.0 sau SAML.

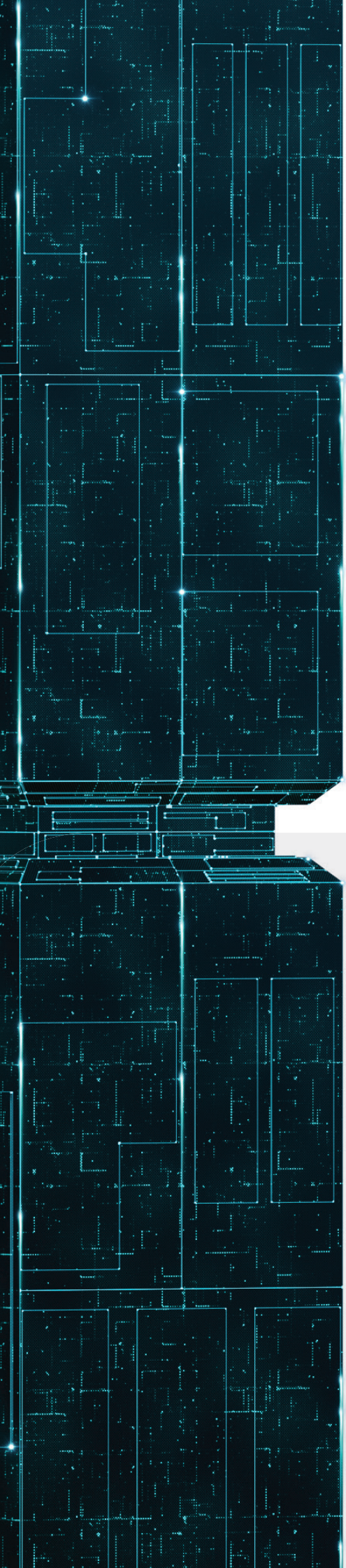
Fiind administrat central prin browser, ESA a fost proiectat să funcționeze pe toate dispozitivele iPhone și Android și, de asemenea, funcționează bine cu mai multe tipuri de autentificare, inclusiv notificări ușor de utilizat, aplicații mobile, token-uri hardware, chei de securitate FIDO și alte metode personalizate (prin intermediul ESA SDK). În paralel, ESA ajută la securizarea datelor companiei și a cloud-ului într-un mod simplu, dar puternic și ajută la îndeplinirea cerințelor de conformitate pentru reglementări precum GDPR.

ÎN CONTEXTUL PANDEMIEI CU COVID-19, PENTRU A AJUTA COMPANIILE SĂ-ȘI PROTEJEZE ÎN MOD CORESPUNZĂTOR SISTEMELE CRITICE ȘI DATELE PERSONALE ESET EXTINDE TRIAL-UL CLASIC DE O LUNĂ DE ZILE A SOLUȚIEI ESA LA 90 DE ZILE.

CITIȚI PREZENTAREA COMPLETĂ ESA

În final, adăugarea criptării full-disk după introducerea MFA, este de asemenea un pas benefic. ESET Full Disk Encryption (EFDE) oferă o criptare puternică a hard disk-urilor de sistem, a partițiilor sau a unităților întregi. Acestea sunt gestionate facil de către consolele de management ESET ESET Security Management Center și ESET Cloud Administrator, îmbunătățind și mai mult securitatea datelor organizației dvs.





INFORMAȚIA ÎNSEAMNĂ PUTERE ... LA FEL ȘI O SECURITATE COMPLETĂ

Diferite tehnici și tactici RDP pot fi, de asemenea, examinate în baza de cunoștințe MITER ATT & CK®. Utilizarea ATT & CK și a altor instrumente (EDR) poate fi foarte utilă pentru examinarea detaliată a amenințărilor cu care se confruntă rețeaua dvs. Instrumente precum ESET Enterprise Inspector (EEI) permit administratorilor de securitate să examineze detecțiile, să solicite direct la ATT și CK KB informații suplimentare și să stabilească alarme personalizate pentru rețeaua ta.

O altă posibilitate legată de amenințările specifice RDP este să realizați detecții (parțiale), dar să rămâneți neprotejat. EDR poate juca, de asemenea, un rol important în scenariile în care pot să nu apară detecții clare. De exemplu, în unele cazuri exploatarea BlueKeep a provocat un crash imediat sistemelor vizate, pentru că s-a dovedit a nu fi construită corect. Deci, pentru ca exploit-ul RDP să funcționeze, poate fi necesar să fie asociat cu un alt exploit, cum ar fi cu o vulnerabilitate a divulgării informațiilor (de exemplu, prin fișiere Flash - php) care dezvăluie adresele de memorie ale kernel-ului, astfel încât acestea să nu mai poată fi ghicite. Acest lucru ar putea reduce probabilitatea unui crash, deoarece exploatarea curentă derulează o manevră de heat spraying. Aceste comportamente specifice pot fi marcate cu reguli personalizate create în cadrul EEI, declanșând în cele din urmă o alarmă și atrăgând atenția administratorului. Informații suplimentare privind nivelul de protecție al rețelei pot fi, de asemenea, furnizate prin testări periodice și verificarea comportamentului suspect prin SIEM, IPS, IDS.

CONCLUZIE

COVID-19 a schimbat modul în care organizațiile funcționează, nu doar temporar pe parcursul pandemiei, ci pentru totdeauna. Angajatorii trebuie să se adapteze nu doar la cerințele angajaților care lucrează de acasă, ci și la modul de lucru din viitor.

Un lucru benefic pe care ni l-a arătat pandemia este că multe joburi în sine și task-uri se pot desfășura fără probleme și într-un mediu de lucru remote, deși anterior se credea că este absolut necesară prezența angajaților la locul de muncă. Dar, pentru ca acest lucru să se întâmple, angajații la distanță trebuie să aibă acces securizat la instrumentele de la birou. ESET oferă o varietate de soluții care pot ajuta companiile să asigure acces securizat la resursele corporative.