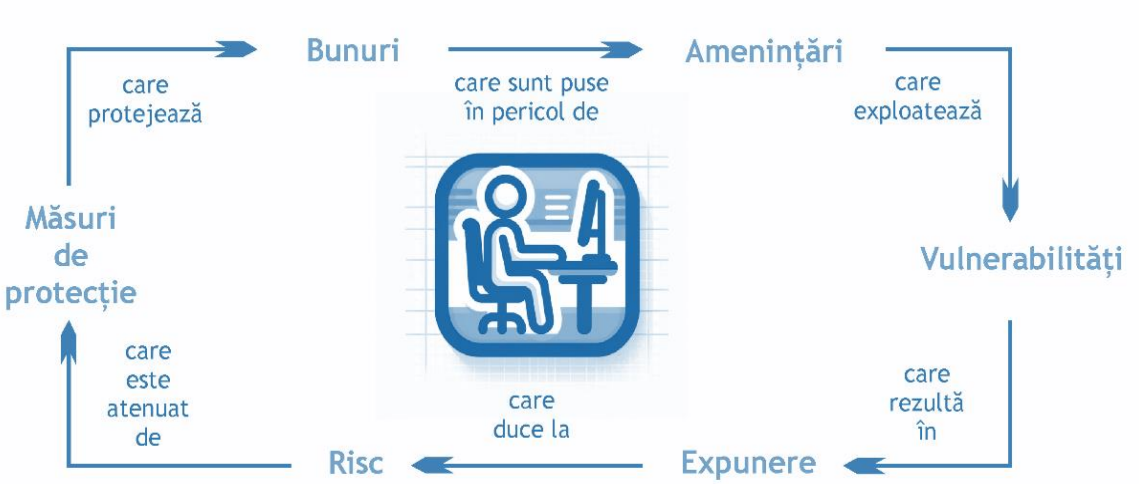
DIRECTORATUL NAȚIONAL
DE SECURITATE CIBERNETICĂ

GHID DE BUNE PRACTICI PENTRU UTILIZAREA APLICAȚIILOR DE ACCES LA DISTANȚĂ

TLP:CLEAR

Introducere

- **Scopul ghidului.** Acest ghid își propune să ofere utilizatorilor o abordare sigură și eficientă în utilizarea aplicațiilor de acces la distanță. Securitatea în utilizarea accesului la distanță este esențială pentru **protejarea sistemelor și datelor** împotriva amenințărilor cibernetice. Indiferent dacă sunteți un profesionist IT care gestionează o rețea mare de dispozitive la distanță sau un utilizator ocazional care accesează PC-ul de la birou printr-o conexiune inițiată de acasă, aceste practici vă vor ajuta să vă asigurați că sesiunile la distanță sunt **sigure**, **stabile** și **eficiente**. Se vor acoperi o serie de subiecte, inclusiv **riscurile, vulnerabilitățile și amenințările** ce pot afecta utilizarea normală a accesului, precum și **configurarea conexiunilor securizate**, **gestionarea accesului utilizatorilor**, **optimizarea performanței**.
- **Ce este accesul la distanță** ? Este o metodă de conectare la servicii, aplicații sau date dintr-o altă locație decât cea în care este păstrată resursa respectivă. Această conexiune permite utilizatorilor accesul la desktop-ul, aplicațiile și la datele computerului de la distanță. Acest mod de lucru poate fi folosit pentru administrarea și gestionarea eficientă a sistemelor, fără a necesita prezența fizică la locația unde acestea se află. Prin această metodă se permite profesioniștilor IT să depaneze problemele sau să monitorizeze resursele fără a se afla în aceeași locație fizică cu dispozitivul sau sistemul ce trebuie remediat/monitorizat.



- **Protocoale de acces la distanță**. Câteva exemple ar fi: **Secure Shell (SSH)**, **Virtual Network Computing (VNC)** sau **Remote Desktop Protocol (RDP)**. În ultimi ani, s-a dezvoltat un număr apreciabil de aplicații de acces la distanță, cele mai multe fiind de tip **remote desktop, bazate pe tehnologii proprietare**, aplicații ce sunt folosite pe scară largă de foarte multe organizații. Cea mai importantă facilitate legată de utilizarea acestora este simplificarea lucrului de la distanță. Deși există caracteristici de securitate native în majoritatea tipurilor de aplicații de acces, simplul act de conectare directă a două dispozitive creează noi provocări de securitate care trebuie abordate, astfel încât operațiunile să se desfășoare în medii sigure.
- **Importanța securității în utilizarea accesului la distanță:** Securitatea în utilizarea accesului la distanță este crucială pentru a preveni **accesul neautorizat**, **interceptarea sau compromiterea datelor** precum și alte amenințări cibernetice. Un serviciu de acces la distanță securizat reduce riscul de compromitere a sistemelor și protejează **confidențialitatea informațiilor**. Deși **aplicațiile de acces la distanță** pot fi o modalitate rapidă de a permite accesul pentru **angajați sau furnizori**, există o serie de provocări de securitate care trebuie luate în considerare înainte de a utiliza acest mod de lucru ca strategie de acces la distanță. Una dintre aceste provocări este că atacatorii continuă să vizeze serviciile de acces la distanță, punând în pericol **rețelele**, **sistemele** și **datele** organizațiilor (de exemplu, agresorii ar putea exploata protocoalele de comunicare pentru a stabili un punct de acces permanent în rețea, pentru a instala ransomware pe sisteme sau pentru a efectua alte acțiuni neautorizate). În plus, există **provocări** în ceea ce privește capacitatea de a configura adecvat **securitatea aplicațiilor de acces la distanță**, pentru a restrânge capacitatea unui agresor de a se deplasa lateral și a compromite și mai multe sisteme și/sau date.

Aplicațiile de acces la distanță (Remote Desktop)

Disponibilitatea multor sisteme de acces la distanță este critică pentru organizații, din cauza creșterii numărului de angajați care lucrează de acasă. Dacă o anomalie a aplicației dedicată lucrului de la distanță ar fi fost considerată acum câțiva ani un risc minor, o astfel de perturbare reprezintă în prezent o **amenințare majoră.**

Care sunt riscurile utilizării aplicațiilor de acces la distanță

În cazul identificării unei vulnerabilități critice în aplicația pentru accesul la distanță, organizațiile se pot confruntata rapid cu o problemă dificilă. Dacă nu aplică măsuri de remediere/limitare, se permite accesul atacatorilor la resursele interne ale organizației. Dacă se intervine și sunt blocate instrumentele de lucru la distanță, continuitatea business-ului organizațiilor poate fi afectată. Pentru o mare parte a companiilor, ambele scenarii pot fi pur și simplu inacceptabile. Este bine să se țină cont de următoarele amenințări atunci când se expun resursele organizației pe internet:

- **Scurgerile de date:** Scurgerile de date pot apărea dacă aplicația nu utilizează criptarea adecvată pentru transmiterea informațiilor între dispozitive sau dacă sistemele sunt compromise.
- **Atacurile de tip phishing** pot viza utilizatorii care accesează aplicații de acces la distanță, în scopul obținerii informațiilor de autentificare ale acestora în mod direct sau prin determinarea acestora să descarce și să ruleze malware.
- **Atacurile de tip Distributed Denial of Services (DDoS) asupra punctelor de acces în rețea.** Acest tip de atac poate perturba operațiunile organizației prin blocarea sau îngreunarea accesului la sistemele/resursele acesteia.
- **Utilizarea aplicațiilor de acces la distanță poate fi o poartă de intrare pentru ransomware**, programe ce pot cripta datele și solicita răscumpărare pentru recuperarea lor, sau alte tipuri de malware.

Mai există, de asemenea, alte scenarii care prezintă diferite riscuri. Exemplele includ suprasolicitarea cauzată de creșterea puternică a numărului de utilizatori, o deficiență a numărului de licențe/conturi sau perturbări neintenționate ale sistemelor de bază.

Aplicațiile dedicate lucrului la distanță sunt foarte atrăgătoare pentru atacatorii cibernetici, deoarece:

- **Nu declanșează întotdeauna instrumentele de securitate.** Aplicațiile de acces la distanță sunt adesea utilizate în scopuri legitime, astfel încât, în general, se integrează în mediu și nu declanșează **apărarea antivirus (AV)**, **antimalware** sau **Endpoint Detection and Response (EDR)**. Aplicațiile **Remote Management and Monitoring (RMM)** sunt semnate cu certificate valide de semnare a codului, emise de autoritățile de certificare de încredere, și este puțin probabil ca acestea să fie considerate suspecte de către aplicațiile AV și EDR. De cele mai multe ori, calea de instalare a aplicației RMM este exclusă din inspecția EDR.
- **Nu necesită dezvoltare extinsă a funcționalității.** Accesul la distanță oferit de aplicații permite atacatorilor cibernetici să eludeze necesitatea de a utiliza sau crea programe malware personalizate, cum ar fi **troienii de acces la distanță (RAT)**. Modul în care aplicațiile de acces la distanță sunt utilizate în mod legitim de administratorii de rețea este similar cu modul în care RAT sunt utilizate de către agresori.
- **Pot permite agresorilor cibernetici să ocolească politicile de control al gestionării aplicațiilor**. Cât timp poate fi necesară ocolirea unor măsuri de securitate, aplicațiile de acces la distanță pot fi descărcate ca **executabile portabile autonome**, ce permit atacatorilor să ocolească atât cerințele privind drepturile de administrator cât și politicile de control al gestionării aplicațiilor.

Notă: Executabilele portabile se lansează în contextul **utilizatorului fără drepturi de instalare**. Deoarece utilizarea executabilelor portabile adesea nu necesită drepturi de administrator, acestea pot permite executarea altor programe neaprobate. Atacatorii pot rula un executabil portabil cu drepturi de utilizator local pentru a ataca alte dispozitive vulnerabile din intranetul local sau pentru a stabili **accesul persistent** ca serviciu local pentru utilizatori.

- **Ar putea permite atacatorilor să ocolească regulile firewall-ului**. Pe lângă ocolirea controalelor de gestionare a aplicațiilor, multe aplicații de acces la distanță

utilizează **criptarea end-to-end**. Acest lucru ar putea permite unui atacator să descarce fișiere care, de obicei, ar fi detectate și blocate la nivel de firewall.

- **Pot facilita multiple intruziuni cibernetice**. Aplicațiile de acces la distanță permit atacatorilor să gestioneze mai multe intruziuni simultan. În plus, brokerii de acces au capacitatea de a vinde accesul la rețea unui număr variat de entități ostile, facilitând astfel intruziuni multiple în aceeași rețea și extinderea acoperirii și capacităților acestora.

Care sunt aplicațiile de acces la distanță cele mai utilizate

Conform ierarhiei furnizate de **techradar.com** cele mai utilizate 12 aplicații de acces la distanță sunt următoarele, cu mențiunea că organizațiile pot alege orice aplicație disponibilă, în funcție de nevoile acestora și bugetul disponibil pentru astfel de achiziții:

LogMeIn Pro[1]	**TeamViewer**[2]	**Remote Desktop Manager**[3]
Splashtop[4]	**Microsoft Desktop Services**[5]	**Chrome Remote Desktop**[6]
Zoho Assist[7]	**ISL Online**[8]	**Parallels**[9]
AnyDesk[10]	**Remote Utilities for Windows**[11]	**VNC Connect**[12]

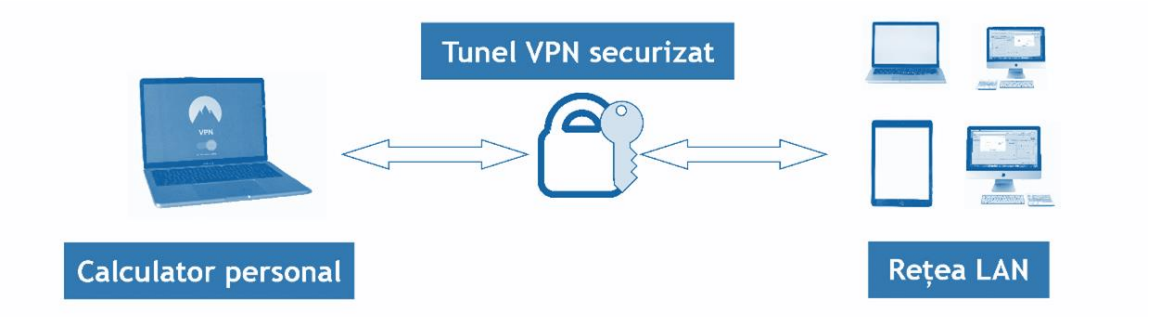
Este esențial ca administratorii IT să fie familiarizați cu comportamentul de bază al unei aplicații de acces la distanță pentru a recunoaște **comportamentul anormal** și pentru a detecta utilizarea anormală și rău intenționată. Administratorii IT ar trebui să coreleze activitatea detectată cu alte comportamente suspecte pentru a reduce rezultatele fals pozitive.

Rețeaua Virtuală Privată

Virtual Private Network (VPN) este o tehnologie care permite crearea unei conexiuni securizate între client și un server VPN. Această tehnologie este esențială pentru sporirea securității și confidențialității datelor transmise prin internet, devenind esențială în utilizarea rețelelor publice nesigure, precum cele din aeroporturi sau cafenele, sau în cazul conexiunilor Wi-Fi slab protejate. Un VPN funcționează prin criptarea traficului de internet, astfel încât informațiile să nu poată fi interceptate de către terți. De asemenea, VPN-ul ascunde adresa IP a dispozitivului personal, făcându-l mai dificil de urmărit pentru site-uri web și servicii online care colectează date despre activitatea online.

De ce este utilă folosirea conexiunilor VPN

- **Securitatea în remote work (telemuncă)**: Conexiunile VPN permit angajaților să se conecteze la rețeaua organizației în mod securizat chiar și atunci când lucrează de acasă sau de la distanță, prin aceasta asigurându-se un nivel adecvat de protecție al datelor organizației.
- **Securitatea conexiunii:** VPN-urile criptează datele transmise între dispozitivul utilizatorului și serverul VPN, oferind astfel o conexiune sigură, cu un grad ridicat de protecție împotriva interceptării datelor transmise de către actorii malițioși. În contextul conexiunilor VPN, criptarea end-to-end se referă la procesul de criptare și decriptare a datelor la ambele capete ale conexiunii VPN: la dispozitivul sursă (utilizator) și la serverul VPN.
- **Ascunderea adresei IP:** VPN-urile ascund adresa IP reală a utilizatorului, înlocuind-o cu adresa IP a serverului VPN. Acest lucru ajută la menținerea anonimatului și la protejarea identității online.
- **Protecția împotriva dezvăluirii adresei IP:** Unele VPN-uri oferă funcționalități pentru a preveni scurgerile de adrese IP, asigurându-se că adresa IP reală utilizată nu este dezvăluită accidental.
- **Accesarea conținutului geografic restricționat:** VPN-urile permit utilizatorilor să acceseze conținut online care ar putea fi restricționat în anumite regiuni geografice prin oferirea unei adrese IP dintr-o altă locație.
- **Securizarea conexiunilor Wi-Fi publice:** VPN-urile oferă o modalitate mai sigură pentru utilizarea rețelelor Wi-Fi publice, protejând datele împotriva potențialelor amenințări de securitate astfel încât să se poată asigura un mediu de lucru securizat.
- **Protecția împotriva atacurilor "Man-in-the-Middle" (MitM):** VPN-urile adaugă un strat suplimentar de securitate, protejând împotriva atacurilor MitM, în care un atacator interceptează și modifică comunicațiile dintre utilizator și server.



- **Nivel de autentificare de o complexitate ridicată, cu ajutorul certificatelor digitale:** Unele soluții VPN acceptă autentificarea cu ajutorul certificatelor digitale pentru clienții care încearcă să acceseze VPN-ul, prin utilizarea unui smartcard/token, aceasta fiind o formă mai puternică de autentificare decât utilizarea parolelor. Oricând este posibil, utilizați autentificarea certificatului client, astfel încât VPN-ul să interzică conexiunile de la clienții care nu prezintă certificate valide și de încredere.

Cât de sigură este utilizarea conexiunilor VPN

- **Niciun software nu este 100% lipsit de vulnerabilități**. Pe măsură ce se adaugă noi funcționalități și tehnologia continuă să evolueze, vor apărea vulnerabilități ce pot fi exploatate. Vulnerabilitățile pot fi în codul aplicației VPN sau în platforma pe care rulează software-ul VPN.
- **Utilizarea unui VPN poate duce la o scădere a vitezei de conexiune** prin criptarea și rutarea traficului prin serverele VPN. Acest lucru poate afecta performanța, în special în ceea ce privește descărcarea și încărcarea de date. Cu cât criptarea traficului este mai puternică cu atâta viteza de transmitere a datelor este mai redusă.

- **Unele conexiuni VPN pot avea scurgeri de date Domain Name Server (DNS)**. Toate serviciile VPN vor stabili o conexiune criptată între client și server dacă sunt configurate corect. Cu toate acestea, dacă "solicitările" DNS realizate nu sunt, de asemenea, gestionate de VPN, atunci un atacator poate afla ce site-uri web au fost vizitate. Este importantă verificarea periodică a funcționării VPN-ului și folosirea instrumentelor adecvate pentru a testa posibilele scurgeri.
- **Un VPN poate fi vulnerabil la atacurile distribuite de tip DDoS** dacă serverele sale nu dispun de resurse suficiente pentru a face față unui volum crescut de trafic, aceasta fiind o situație comună pentru serviciile VPN gratuite.

Aplicațiile VPN cele mai utilizate

- **VPN Center** furnizează un top al celor mai utilizate servicii VPN, din care prezentăm 6, alegerea lor rămânând strict opțiunea fiecărei organizații în funcție de funcționalități, cerințe și bugetul alocat.

NordVPN[13]	**ProtonVPN**[14]	**SurfsharkVPN**[15]
CyberghostVPN[16]	**TunnelBearVPN**[17]	**ExpressVPN**[18]

15 bune practici pentru asigurarea unui nivel adecvat de securitate

1. Utilizarea metodelor puternice de autentificare

Acolo unde este posibil se va adăuga o metodă suplimentară de autentificare înainte de a stabili o conexiune de acces la distanță. Utilizarea autentificării cu doi factori sau multifactor: implementarea uneia sau mai mulor metode suplimentare de autentificare, pe lângă utilizarea parolelor conturilor de acces, acolo unde este posibil. Pentru sistemele care folosesc conexiunea de tip RDP se va activa opțiunea de securitate **Network Level Authentication** (NLA).

2. Gestionarea conturilor de utilizator și a permisiunilor acestora

Se va limita accesul utilizatorilor și se vor acorda permisiuni pentru acces la distanță doar celor care au neapărat nevoie. Implementarea principiului celui mai mic privilegiu prin care se asigură utilizatorilor permisiunile minime și necesare pentru rolul lor. Eliminarea conturilor care nu mai sunt active/necesare.

3. Configurarea securizată a parametrilor conexiunilor de acces la distanță

Modificarea porturilor de acces la distanță implicite (de ex: 3389) poate ajuta la evitarea atacurilor automate. Aceasta este doar o măsură de securitate prin obfuscare. Se vor stabili limite de timp pentru sesiuni, programând închiderea automată a sesiunilor după o anumită perioadă de inactivitate pentru un control mai eficient al acestora și o protecție mai bună. Se vor dezactiva funcțiile **Clipboard Redirection** și **Drive Mapping**.

4. Utilizarea conexiunilor de rețea securizate

Folosirea VPN-ului pentru a cripta traficul între punctele de conexiune și asigurarea implementării protocoale securizate, cum ar fi **OpenVPN** ,**WireGuard** sau **IKEv2/IPsec**, și evitarea protocoalele mai puțin sigure, de ex. **Point-to-Point Tunneling Protocol (PPTP) sau Layer 2 Tunneling Protocol (L2TP).** Pentru filtrarea conexiunilor de tip RDP se va implementa un gateway de tip Remote Desktop.

5. Implementarea straturilor de securitate

Prin configurarea regulilor de firewall se va restricționa accesul de la distanță la anumite adrese IP sau rețele, blocând accesul la distanță din zone geografice suspecte. Utilizarea sistemelor de detectare a intruziunilor - **Intrusion Detection Systems** (IDS) - pentru a monitoriza activitățile suspecte. Restricționarea accesului la distanță doar la rețelele interne ale organizației, **dacă este posibil**, evitând expunerea inutilă pe internet a sistemelor critice/importante.

6. Utilizarea parolelor puternice pentru autentificare

Parolele de acces ar trebui să includă o combinație de litere majuscule și minuscule, numere și simboluri, pentru a mări complexitatea și a reduce riscul atacurilor de tip brute-force reușite. Este recomandată utilizarea unei combinații de litere mici (a-z), litere mari (A-Z), cifre (0-9) și caractere speciale (!, @ etc.) – de exemplu: !miplac35am3rglaMunt3 (**Îmi place sa merg la munte**).

Se va evita utilizarea cuvintelor comune, numelor proprii sau informațiilor personale ce pot fi ușor de ghicit. O parolă puternică ar trebui să aibă cel puțin **12 caractere**, cu cât este mai lungă, cu atât este mai dificil de spart. Se recomandă utilizarea unei parole de cel puțin **16 caractere** pentru o securitate sporită.

7. Implementarea unui program de instruire a utilizatorilor și exerciții de phishing

Aceste activități sunt necesare pentru a crește gradul de conștientizare al utilizatorilor cu privire la riscurile de a vizita site-uri web suspecte, de a face clic pe linkuri suspecte și de a deschide atașamente suspecte. Un grad de conștientizare ridicat pentru aceste tipuri de amenințări poate fi o măsură preventivă eficientă.

8. Utilizarea de măsuri de protecție pentru scripturi cu propagare în masă

Se va utiliza un proces de aprobare/validare a acestora. De exemplu, dacă un cont încearcă să trimită comenzi către zece sau mai multe dispozitive într-o oră, redeclanșați protocoalele de securitate, cum ar fi autentificarea multifactor (MFA), pentru a avea certitudinea că sursa este legitimă și acțiunile desfășurate sunt în permanent control.

9. Examinarea jurnalelor cu date complete (log-uri)

Se vor urmări informații despre executarea binară, tipurile de solicitări, adresele IP și data/ora, referitoare la executarea aplicațiilor de acces la distanță pentru a detecta utilizarea anormală a programelor care rulează ca executabil portabil. Jurnalele de securitate joacă un rol esențial în identificarea și investigarea incidentelor de securitate, asigurarea integrității sistemului și menținerea unui mediu informatic sigur.

10. Stabilirea unei frecvențe regulate în aplicarea patch-urilor

Se vor prioritiza aplicațiile și sistemele care au acces direct la sau sunt accesate de pe Internet, inclusiv pentru accesul la distanță, administrarea serverelor și agenților aferenți diverselor aplicații. Frecvența realizării acestor activități trebuie stabilită astfel încât perioada de timp scursă de când patch-urile sunt disponibile și până când sunt implementate să fie cât mai scurtă. Automatizarea acestui proces este de dorit pentru sistemele cu un număr semnificativ de dispozitive.

11. Utilizarea de variante alternative pentru accesul la distanță

Se pot utiliza și următoarele tipuri de aplicații: **Virtual Desktop Infrastructure (VDI)**, **Remote Desktop Server (RDS)** și **Virtual Network Computing (VNC)** atunci când se dorește virtualizarea unei rețele.

12. Activarea unui Firewall pentru Aplicații Web (WAF)

Acesta ar trebui să fie compatibil cu traficul TLS VPN pentru a proteja aplicațiile de acces la distanță prin filtrarea și monitorizarea traficului HTTP. Chiar dacă această măsură de atenuare este importantă, se recomandă administratorilor IT să o testeze înainte de a o implementa într-un mediu de producție, fiind cunoscut faptul că WAF-urile perturbă funcționarea normală a aplicațiilor de acces la distanță.

13. Aplicarea de măsuri specifice unei arhitecturi Zero Trust

Se va urmări separarea conexiunilor seturilor de date aparținând furnizorilor de servicii/produse (și a serviciilor, acolo unde este cazul) unele de altele – **precum și de rețelele interne ale organizației** – astfel încât, în cazul unui atac malițios reușit, să se poată limita impactul asupra resurselor organizației.

14. Asigurarea copiilor de rezervă a datelor

Acestea sunt un mod eficace de redresare în caz de dezastre sau în cazul unui atac ransomware reușit. Copiile trebuie realizate în mod regulat, ori de câte ori este posibil, fiind păstrate într-un mediu separat de cel al producției. Criptarea copiilor de rezervă asigură securitatea acestora, în special, în cazul în care acestea vor fi mutate dintr-un loc în altul.

15. Efectuarea periodică de evaluări formale pentru amenințările și riscurile potențiale

Organizațiile trebuie să înțeleagă care sunt amenințările și riscurile ce pot afecta operațiunile desfășurate. Procesul presupune identificarea bunurilor (assets) care au nevoie de protecție, a amentințărilor potențiale precum și a vulnerabilităților asociate cu bunurile organizației pentru înțelegerea mai bună și gestionarea mai eficientă a riscurilor.

Recomandări pentru administratorii de securitate cibernetică

Utilizarea de aplicații care să ofere un ghid de securitate on-line. Administratorii de securitate cibernetică trebuie să aibă în vedere implementarea de soluții de conectare la distanță și VPN ce au instrucțiuni de instalare și configurare a aplicației în mediile hardware disponibile în cadrul organizației, instrucțiuni de instalare, configurare și utilizare a aplicațiilor și serviciilor pe terminalele client și să le urmeze întocmai. Furnizorii de astfel de aplicații trebuie să aibă ghiduri de securitate cibernetică iar acolo unde este disponibil serviciul de instalare al aplicațiilor, este recomandat ca acesta să fie folosit.

Verificarea condițiilor contractuale de securitate a aplicațiilor și serviciilor achiziționate. Raportul comercial dintre furnizorii de aplicații de conectare la distanță și beneficiari trebuie să aibă stipulate clauze de garantare a unui nivel de securitate a aplicației. Fiecare furnizor trebuie să își ia toate măsurile necesare pentru a evita breșele de securitate ce pot apărea în cadrul mediului on-line de funcționare al aplicațiilor de conectare la distanță. Serverele furnizorilor, site-urile de vânzare sau portalurile de conectare web trebuie să asigure o conectare în siguranță a tuturor utilizatorilor. Furnizorii trebuie să aibă stipulat public asumarea implementării unor măsuri de securitate cibernetică cu privire la instruirea

angajaților, investirea în cercetarea și dezvoltarea de noi tehnologii de îmbunătățire a securității cibernetice a aplicațiilor oferite și serviciilor aferente.

Raportarea activităților suspicioase ce pot constitui un incident de securitate cibernetică. În cazurile în care se constată tentative de acces neautorizat la sistemele sau datele organizației, întreruperi neintenționate sau atacuri de tip (D)DoS asupra rețelei de acces la internet, phishing sau instalare aplicații malițioase, detalii relevante despre acestea se vor raporta către Directoratul Național de Securitate Cibernetică (DNSC) prin formularul online de pe pagina de web www.dnsc.ro, prin email la adresa alerts@dnsc.ro sau prin apelare la **1911**, numărul unic de urgență la nivel național dedicat raportării incidentelor de securitate cibernetică.

Acest ghid a fost realizat de experții DNSC: **Dan Andrieș, Cristian Nistor, Lucian Păuc, Teodor Vergu.**

Resurse utile

Gestionarea sistemelor de lucru la distanță: recomandări pentru organizații

Ghid privind securitatea cibernetică pentru IMM -uri

Conectarea la o rețea VPN în Windows

Ghid practic pentru OSE

Guide to securing remote access software

What is Remote Access? Definition and How It Works

Selecting and Hardening Remote Access VPN Solutions

Thechradar – Best Remote Desktop Software

VPN Center – Best VPN Services

Referințe

[1] LogMeIn Security: An In-Depth Look

[2] TeamViewer Security Handbook

[3] Remote Desktop Manager Security Dashboard

[4] Splashtop Enterprise: Administrator Guide

[5] Security guidance for remote desktop adoption

[6] Protective Measures to Avoid CRD Security Risks

[7] Securing your Zoho Assist account

[8] ISL Online Security Tips

[9] Parallels Security Compliance

[10] AnyDesk Security Tips

[11] Remote Utilities for Windows Security

[12] VNC Connect Security

[13] NordVPN Security Features

[14] ProtonVPN Secure Core

[15] SurfsharkVPN Trust Center

[16] CyberGhost VPN & Windows Security Suite

[17] TunnelBearVPN - How to Work From Home With TunnelBear

[18] ExpressVPN Trust Center