Agència Nacional de Ciberseguretat d'Andorra

Conscienciació en ciberseguretat

Protecció i Seguretat en els dispositius Endpoint

Què significa el terme ENDPOINT?

Per explicar què és la Seguretat Endpoint, primer hem d'esclarir quin és el significat del concepte «Endpoint».

«Endpoint» fa referència a tot aquell dispositiu reconegut i autoritzat que es connecta de manera **remota** a la **xarxa interna** de l'empresa o organització, ja siguin portàtils, *smartphones*, tauletes i altres dispositius que formen part de la Internet de les coses.

La Seguretat Endpoint és considerada per alguns tècnics com una branca de la Ciberseguretat aplicada a aquells dispositius que es connecten de forma remota a la xarxa de l'organització, imposant-se sobre ells una sèrie de **mesures tècniques** i de **seguretat** que tenen com a objectiu protegir aquests dispositius en qüestió de possibles atacs i intrusions a la xarxa interna de l'organització.

Dada important a destacar i que dona lloc a nombroses confusions:

No hem de confondre la Seguretat Endpoint amb els Sistemes EDR, és a dir, *Sistemes d'Endpoint Detection and Response.* Un Sistema EDR pot ser només una de les múltiples solucions o opcions de seguretat Endpoint establertes per l'organització per tal de protegir la seva xarxa i infraestructura de les possibles amenaces i atacs externs.

Dispositius als quals afecta la Seguretat pels Endpoint:

Els Sistemes de Seguretat pels Endpoint protegeixen aquests punts finals de les xarxes internes de les organitzacions de possibles amenaces de Ciberseguretat externes que es puguin produir com ara: virus, atacs de hackers, cucs informàtics, etc.

La Seguretat dels Endpoint ha evolucionat considerablement, ja que hem passat de tenir el típic i tradicional antivirus, a tenir sistemes molt més avançats que tenen la capacitat de proveir una protecció molt més **completa i integra, en temps real i en múltiples dispositius alhora.**

Com ja hem esmentat, els **dispositius** que es veuen afectats per la Seguretat Endpoint són aquells que tenen la capacitat de connectar-se de manera **remota** a la **xarxa interna** de l'organització.

Aquests dispositius comprenen tant els que fan servir els empleats per realitzar les seves tasques professionals, com aquells altres que són necessaris perquè funcioni la pròpia xarxa de l'organització com per exemple: els servidors.

Per què es necessita la Seguretat als Endpoint?

La Seguretat és necessària en un Endpoint perquè aquest és el punt més **VULNERABLE** que existeix dins d'un Sistema Informàtic.

La majoria dels ciberatacs i virus s'introdueixen als servidors informàtics mitjançant un Endpoint mal protegit. Per exemple: es pot enviar un e-mail maliciós a la safata d'entrada de l'ordinador d'un empleat, enviar un programari maliciós que s'amaga darrere d'una descàrrega d'Internet... Totes aquestes accions poden donar lloc a un **atac** important que pogués perjudicar el **rendiment** i la **integritat** dels equips i, fins i tot, la **pèrdua** i **filtració** d'**informació** que és considerada rellevant i clau per a l'organització.

Què hem de fer per assegurar la Seguretat als Endpoint?:

L'objectiu principal d'un Programari de Seguretat Endpoint és protegir els sistemes contra un **Programari Maliciós** com per exemple, un virus o un *spyware* els quals poden instal·lar-se a l'ordinador d'un empleat sense el coneixement i consentiment del mateix.

Una altra raó per la qual la Seguretat als Endpoint és clau, és que, en l'actualitat, la quantitat d'Endpoints dins d'un sistema s'ha multiplicat considerablement gràcies als nombrosos **avenços en la tecnologia**. Per exemple, els mòbils no només es fan servir per realitzar les tasques tradicionals de trucar per telèfon o enviar missatges, sinó que s'han convertit en una eina capaç de realitzar múltiples funcions.

A mesura que els diferents tipus d'Endpoint han anat evolucionant i s'han anat estenent arreu del món, les **solucions de seguretat** que els protegeixen també han hagut d'adaptar-se, millorar i modernitzant-se per tal de poder protegir-los.

Com funciona la Seguretat als Endpoint?

1. Detecció d'amenaces

La principal funció de la Seguretat Endpoint és la **prevenció**, és a dir, la detecció de les amenaces el més aviat possible per tal d'evitar que l'organització pugui ser víctima d'un **ciberatac** el punt d'accés del qual sigui el dispositiu en remot en qüestió.

Imaginem-nos que un empleat ha descarregat i obert un arxiu adjunt que ha rebut mitjançant un correu electrònic i aquest està infectat amb un programari maliciós que després s'ha anat expandint per tota la xarxa.

És, per tant, el fet d'evitar que es produeixin **bretxes de seguretat** als vostres sistemes i a través d'aquests dispositius en qüestió, el que seria la principal finalitat d'aquests sistemes de Seguretat.

Com funciona la Seguretat als Endpoint?

2. Eines habituals d'aquests sistemes de seguretat

Hi ha eines amb les quals es pot reforçar encara més la seguretat dels dispositius Endpoint més enllà dels **antivirus** que, per descomptat, hauria d'estar ja instal·lat als vostres dispositius.

Per exemple, algunes d'aquestes eines vetllen per la Seguretat als Endpoint:

→ **Sistema EDR** (*Endpoint Detection and Response*): Sistema de seguretat que empra diferents eines de detecció i tecnologies per dur a terme una **millor detecció i prevenció automatitzada d'amenaces més complexes**. També, **minimitza l'impacte de l'amenaça** i **l'elimina**.

→ La utilització de **llistes blanques** per restringir la connexió de dispositius a través de xarxes WiFi o IPs que hagin estat autoritzades prèviament. També, aquestes serveixen per **bloquejar correus electrònics de direccions sospitoses o l'accés a webs fraudulentes**.

→ Emprar una **xarxa privada virtual** (VPN) per connectar-se a la xarxa de l'organització i augmentar amb això la seguretat de la mateixa. D'aquesta manera, a ella només podran connectar-se aquells dispositius que estiguin degudament autoritzats i que mantinguin la deguda **confidencialitat** de la informació que es desplaça en una xarxa xifrada.

→ Afegir també els **Firewalls o tallafocs**: Primera línia de defensa contra moltes ciberamenaces i que es fan servir per prevenir l'entrada de possibles *malwares* al sistema.

Com funciona la Seguretat als Endpoint?

2. Eines habituals d'aquests sistemes de seguretat:

→ **Sistema de confiança Zero Trust:** Diferents **nivells d'accés i privilegis**, limitant aquests al mínim i estrictament necessari.

→ **Monitoratge i auditories:** Permeten **controlar i analitzar el comportament d'un usuari a la xarxa interna**, des de que inicia la sessió, fins que es desconnecta, passant per quins arxius ha consultat, què ha descarregat i inclòs quins llocs web ha visitat. D'aquesta manera es poden detectar comportaments inusuals.

→ **Xifratge de dispositius i de memòria externa**: Evitarà que la informació confidencial pugui acabar en mans alienes, en el cas que s'extraviés un equip portàtil.

Conclusió final:

La **prevenció** és essencial per evitar que la xarxa de l'organització sigui víctima de ciberatacs, així que, a banda de les eines que hem analitzat, caldria configurar bé la clau de seguretat de la xarxa per tal d'evitar que qualsevol persona pugui entrar a la WiFi de l'organització.

Característiques d'un bon programari de Seguretat Endpoint

Les solucions de Seguretat d'Endpoint estan disponibles en dos tipus que han estat definits pel lloc on està ubicada la instal·lació: **Models Locals** i **Models basats en el Núvol.**

Característiques

1. Seguretat Endpoint en Models Locals

En aquests casos els sistemes de protecció d'Endpoint són instal·lats dins dels propis servidors de l'organització. Això respon més aviat a polítiques internes empresarials, que a la seguretat que un sistema de Seguretat Endpoint pot donar o necessitar.

2. Seguretat Endpoint en Models basats al Núvol

Per la majoria de les organitzacions, la millor solució per garantir la seguretat als seus Endpoint és el núvol.

Principals beneficis:

- No es necessita instal·lar absolutament res dins dels servidors propis de l'organització.
- No requereixen manteniment i la seva gestió és molt fàcil de realitzar.
- La capacitació, escalament i integracions són molt fàcils de dur a terme.

Per què és important aplicar solucions de Seguretat Endpoint als dispositius emprats a la meva organització?

Aplicar solucions de Seguretat Endpoint en la vostra organització us ajudarà bastant a **minimitzar el risc** de patir diferents tipus de ciberatacs que posarien en perill no només la **confidencialitat** de la informació professional que manegeu per prestar un servei o realitzar una activitat professional i que, evidentment, és clau pel funcionament de l'organització.

Per tant, la no protegir els Endpoint suposaria tant **pèrdues econòmiques**, com **pèrdues de reputació** per l'organització.

Cal tenir en compte que, en moltes ocasions, és molt complicat controlar tots els dispositius que es connecten de forma remota a la xarxa interna de la vostra organització, tot i que cada vegada és més freqüent que les organitzacions inverteixin molt en **formar** als seus empleats i en conscienciar-los en aquestes matèries per tal que puguin reconèixer i evitar **amenaces electròniques.**

Conclusió final:

Reforçar la seguretat Endpoint us ajudarà a **detectar** i **evitar** moltes d'aquestes amenaces o a **minimitzar** i **reduir** el seu impacte.

Seguretat Endpoint i Teletreball

Amb l'augment del **teletreball**, la seguretat Endpoint hauria de ser un **punt clau** a tenir en compte en la ciberseguretat de la vostra organització.

Amb empleats que treballen des de casa i que es connecten, la majoria de les vegades, a **xarxes no segures** o que no compten amb la suficient **seguretat**, reforçar la Seguretat en els dispositius Endpoint podria evitar que la vostra organització pateixin nombrosos atacs de *phishing*, *ransomware*, enginyeria social, amenaces electròniques, etc.

Treballar des de casa pot fer que la gent no estigui suficientment **alerta**, accedint a llocs web que si estiguessin a l'oficina no farien servir o no podrien accedir o, altrament, que es descarreguin arxius sense comprovar prèviament el seu origen.