GUIA BÀSICA DE LA CIBERSEGURETAT A LES EMPRESES

INTRODUCCIÓ

La informació és un dels actius més importants de les nostres empreses i, com a tal, protegir-ne la confidencialitat, integritat i disponibilitat és una de les tasques a les quals hem de dedicar especial atenció. Les conseqüències d'un atac reeixit poden ser fatals per a una empresa de mida petita o mitjana.

Avui, la ciberseguretat es considera una part necessària de qualsevol empresa, i per això cal prendre les mesures que calgui per millorar-la. Entre altres mesures, cal adoptar aquelles destinades a adequar-se a la normativa legal vigent (LOPD, LSSI, etc.), protegir els sistemes i infraestructures de qualsevol atac o amenaça o, amb una visió més integral, posar en marxa un Pla Director de Seguretat.

Aquesta guia vol ajudar les empreses a tenir unes nocions clares de quins són els riscos als quals s'enfronta i què fer per protegir-se'n. També vol oferir consells adreçats a les persones que treballen a les empreses, perquè elles són una part imprescindible en l'estratègia de ciberseguretat.

ATACS DELS QUALS T'HAS DE PROTEGIR

ENGINYERIA SOCIAL I CORREU ELECTRÒNIC, L'ORIGEN DE MOLTS INCIDENTS

Enginyeria social: utilitzar diferents tècniques de manipulació psicològica amb l'objectiu d'aconseguir que les víctimes revelin informació confidencial o realitzin qualsevol d'acció que pugui beneficiar al ciberdelinqüent.

Exemple: revelar informació confidencial o instal·lar programari maliciós.

Captura d'un correu fraudulent imitant la identitat de Correos.

El correu electrònic, principal mitjà de comunicació fraudulenta?

El correu electrònic pot ser una eina perillosa, ja que moltes vegades les tasques es fan de forma mecànica, la qual cosa pot provocar infeccions per *malware* o accessos a pàgines web fraudulentes.

Algunes de les tècniques que utilitzen els ciberdelinqüents per crear campanyes malicioses són:

- ***E-mail spoofing:*** falsejar l'adreça del remitent (impersonalització).
- **Falsejar enllaços:** enllaços falsificats que simulen enllaçar a un lloc web legítim quan en realitat no és així.
- **Adjuntar documents maliciosos:** adjunts maliciosos que simulen fitxers legítims. Aquests arxius poden estar comprimits per camuflar-se.

Detectar un atac per enginyeria social

- **Remitents desconeguts:** cal analitzar l'adreça del remitent. Els ciberdelinqüents utilitzen comptes de correu que no tenen res a veure amb l'entitat a què suposadament representen.
- **Remitents falsejats:** cal analitzar les capçaleres del correu i comprovar el nom del domini; una simple lletra podria ser l'origen d'un incident de seguretat.
- **Comunicacions impersonals:** les comunicacions fraudulentes rebudes per correu electrònic són impersonals.
- **Adjunts sospitosos:** cal comprovar prèviament l'extensió del fitxer adjunt i vigilar amb les extensions .exe, .vbs, .msi, .docm, .xlms o .pptm. Cal vigilar també amb els fitxers comprimits que continguin un arxiu amb alguna de les extensions anteriors.
- **Revisar l'ortografia i l'expressió:** la presència de faltes ortogràfiques o errors gramaticals és un símptoma de comunicació fraudulenta.
- **Enllaços falsejats:** els correus electrònics moltes vegades contenen enllaços que redirigeixen l'usuari a una web fraudulenta.
- **Firmes i altres elements a la plantilla de correu:** cal identificar elements comuns, com la signatura de la part inferior o els avisos legals. Si aquesta firma o el paràgraf legal és diferent o no hi és, podria ser símptoma de què aquesta comunicació és fraudulenta.

FRAU DEL DIRECTOR (*SPEAR PHISHING*, O FRAU DEL CEO)

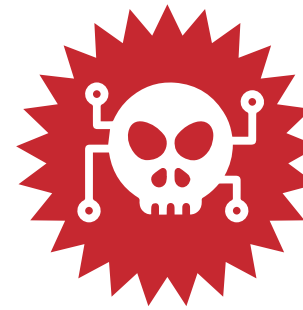
Consisteix en un atac dirigit en contra d'una víctima de la qual s'ha recopilat informació prèviament amb l'objectiu de fer l'atac més creïble.

Se suplanta la identitat d'un alt directiu i se sol·licita a un treballador realitzar una transferència de diners. Les comunicacions es fan per correu electrònic i utilitzant adreces falsejades. Fins i tot s'utilitza l'adreça legítima del directiu que, prèviament, s'ha compromès. Moltes vegades la sol·licitud de transferència s'acompanya d'una petició d'urgència i confidencialitat.

Detectar un atac de frau del CEO

- **Verificar per un altre mitjà de comunicació:**
  1. **No s'ha de respondre mai el correu rebut**
  2. **Cal verificar la sol·licitud per un altre canal de comunicació (trucada telefònica o missatgeria instantània).**
- **Comprovar el remitent:** cal analitzar la capçalera del correu i comprovar el nom del domini; una simple lletra podria ser l'origen d'un incident de seguretat.
- **Revisar sol·licituds urgents i confidencials:** qualsevol sol·licitud que vagi acompanyada d'urgència i confidencialitat ha de posar en alerta els usuaris, ja que pot tractar-se d'un intent de frau.
- **Revisar l'ortografia i l'expressió:** la presència de faltes ortogràfiques o errors gramaticals és un símptoma de comunicació fraudulenta.
- **Firmes i altres elements a la plantilla de correu:** cal identificar elements comuns, com la signatura de la part inferior o els avisos legals. Si aquesta firma o el paràgraf legal és diferent o no apareix podria ser símptoma de què aquesta comunicació és fraudulenta.

RANSOMWARE



És un *malware* que afecta la informació impedint el seu accés, generalment xifrant-la i demanant un rescat econòmic als afectats a canvi de poder recuperar-ne l'accés.

Les infeccions per *ransomware* es produeixen per dues vies diferents:

- **Campanyes de *malware* a través del correu electrònic.**
- **Vulnerabilitats o configuracions de seguretat deficients.**

Evitar un atac de *ransomware*

- **Precaució amb adjunts en correus electrònics i enllaços a pàgines externes:** cal seguir les mateixes recomanacions que en les campanyes d'enginyeria social. Algunes extensions de fitxers potencialment fraudulents són .exe, .msi o .vbs
- Arxius ofimàtics amb macros: .docm, .xlsm, .pptm, .doc, .xls, .ppt, .docx, . xlsx o .pptx
    - Qualsevol arxiu comprimit que contingui alguna de les anteriors extensions.
    - ***Software* actualitzat i configuracions de seguretat robustes:** tot el programari de l'empresa ha d'estar sempre actualitzat a l'última versió disponible. També és recomanable utilitzar contrasenyes robustes i evitar utilitzar noms d'usuari comuns o genèrics, com a administrador, nom de l'empresa, etc.
- **Eines *antiransomware*:** fer servir eines específiques que monitorin la xarxa i els dispositius empresarials detenint i bloquejant els processos de xifratge.

Com actuar en cas de patir un atac de *ransomware*

- **Aïllar l'equip o equips infectats de la xarxa** principal de l'organització.
- **Clonar els discs dels dispositius infectats.** D'aquesta manera es podrà mantenir el disc en el seu estat original i intentar recuperar les dades sobre la còpia.
- **Desinfectar els dispositius afectats i el disc clonat** per intentar recuperar els arxius xifrats.
- **Intentar recuperar els arxius xifrats** en el disc clonat prèviament desinfectat. En cas de disposar d'una còpia de seguretat s'ha de restaurar utilitzant la més recent i lliure de modificacions malicioses.
- **Utilitzar un disc nou o formatat** i una instal·lació neta del sistema operatiu i restaurar la còpia de seguretat més recent, anterior a la infecció.

Captura de pantalla del *ransomware wannacry*.

ATACS CONTRA LA PÀGINA WEB CORPORATIVA

Els incidents de seguretat poden derivar en diverses situacions que poden comprometre la seguretat i privacitat de l'empresa i els seus clients.

- **Fugues d'informació:** un incident que afecti la pàgina web corporativa pot originar una fuga tant d'informació confidencial de l'empresa com del seu personal i clients.
- **Denegacions de servei:** una denegació de servei o DOS (*Denial of Service*) pot deixar un servidor inoperatiu.
- **Com a origen d'un altre incident de seguretat:** quan es vulnera la seguretat de la pàgina web corporativa es poden arribar a comprometre altres serveis de l'organització, com el correu electrònic, ordinadors, dur a terme atacs de tipus *ransomware*, etc.
- ***Defacement*:** consisteix a canviar l'aparença de la pàgina web corporativa per una altra a elecció del ciberdelinqüent com a reivindicació política, presumir o simplement danyar la reputació de l'organització.
- **Com a eina per atacar altres usuaris:** vulnerar la seguretat de pàgines web legítimes i utilitzar-les com a trampolí per perpetrar altres fraus.

Evitar els atacs contra la pàgina web corporativa

- **Certificat SSL:** protegeix les comunicacions entre la pàgina web corporativa i el dispositiu de l'usuari, evitant que es pugui robar la informació en trànsit. També serveix per identificar la web de forma inequívoca.
- **Actualitzacions de seguretat:** la gran majoria de pàgines web estan dissenyades utilitzant gestors de contingut o CMS (*Content Management System*, com Wordpress o Drupal).

Aquests CMS publiquen regularment actualitzacions de seguretat que corregeixen vulnerabilitats descobertes. Sempre s'ha de comptar amb l'última versió disponible del CMS. També s'han de tenir actualitzats la resta de components que conformen el gestor, com són els *plugins* i temes utilitzats.

- **Contrasenyes robustes:** les contrasenyes d'accés han de ser tan robustes com sigui possible. És per això que han d'incloure majúscules, minúscules, números i símbols i tenir una longitud mínima de 8 caràcters.
- **Còpies de seguretat:** s'han de realitzar còpies periòdiques, emmagatzemar-les en un entorn segur i comprovar que és possible la seva restauració.
- **Sistemes *captcha*:** aquests sistemes impedeixen que els *bot* o programes automatitzats puguin interactuar amb determinades parts de la web.
- **Monitoratge de tràfic:** monitorar el tràfic serveix per identificar possibles indicis de ciberatac.
- **Sistemes alternatius:** permeten continuar oferint el servei web als clients i treballadors en cas d'incident de seguretat o fallada del sistema.
- **Proveïdor de seguretat extern:** escollir un proveïdor de seguretat dota d'un extra de seguretat a la web i permet reduir les conseqüències en cas de patir un incident de seguretat.
- **Compliment legal i normatiu:** la pàgina web ha de complir amb la legalitat vigent. Per això ha de tractar les dades personals d'acord amb la Llei Orgànica de Protecció de Dades i Garantia de Drets Digitals o LOPDGDD, la Llei de Serveis de la Societat de la Informació o LSI i la Llei de Propietat Intel·lectual o LPI. A més a més, haurà de complir qualsevol mena de normativa vigent que pugui afectar l'activitat de l'empresa.

ESTABLIR UNA ESTRATÈGIA DE CIBERSEGURETAT: EL PRIMER PAS ÉS AVALUAR EL RISC

Abans d'implantar qualsevol mesura cal conèixer el nivell de seguretat de l'organització. Cal realitzar periòdicament auditories de seguretat de la informació, que consisteixen en un estudi detallat de tota l'estructura dels sistemes d'informació de l'organització. Les porten a terme els professionals i el seu objectiu és avaluar i millorar la seguretat, l'eficàcia i l'eficiència dels processos productius. Aspectes que cal considerar:

- Protecció **antivirus**
- Protecció **antispam** i de filtratge de continguts
- Prevenció de **fugida de dades** (DLP)
- Administració de **permisos** d'usuaris i **accessos** a serveis
- Prevenció del **frau**
- Seguretat dels **dispositius mòbils**
- Gestió automatitzada d'**actualitzacions del programari**
- Detecció de **vulnerabilitats**
- Gestió unificada d'amenaces (UTM)
- Monitoratge de **l'ús dels recursos** informàtics i de xarxa
- Monitoratge i anàlisi d'**esdeveniments de seguretat** en temps real (SIEM)

- Compliment **legal**

- En la majoria dels casos, cal sol·licitar al proveïdor de serveis tecnològics la realització d'aquestes auditories. N'hi ha diverses en funció del tipus d'anàlisi que facin: **test de penetració.** Conjunt de proves a què se sotmet una aplicació, servei o sistema amb l'objectiu de trobar buits o errors a través dels quals seria possible aconseguir accés no autoritzat a informació de l'empresa.

- **Auditoria de xarxa**. Cal analitzar la xarxa de l'empresa a la recerca de ports oberts, recursos compartits, serveis o electrònica de xarxa (*router, switch,* etc.). En aquestes auditories s'utilitzen eines que permeten fer la catalogació de les infraestructures connectades a la xarxa o, fins i tot, detectar versions de dispositius insegurs, versions de programari o la necessitat d'instal·lar actualitzacions.

- **Auditoria de seguretat perimetral.** Destinada a determinar el nivell de seguretat de les barreres que protegeixen la xarxa de comunicacions d'una organització especialitzada a detectar errors de seguretat des del punt de vista exterior.

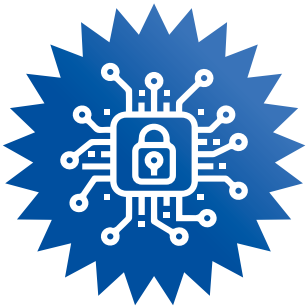
- **Auditoria web.** Analitza els errors de seguretat o les vulnerabilitats que afecten el funcionament d'una pàgina web.

- **Auditoria forense.** Auditoria posterior a un incident de seguretat per identificar les causes que l'han produït. Té com a objectiu demanar i preservar les proves o evidències d'un incident per, després de la seva posterior anàlisi, saber què i com ha passat, aprendre'n i depurar les possibles conseqüències legals.

Actualment, gràcies als productes i serveis que es poden trobar al mercat de seguretat, aquesta tasca s'ha simplificat de manera significativa. Però en general, és necessari que les realitzi personal especialitzat.

És molt recomanable conèixer el nivell de seguretat de l'organització abans de dissenyar i implementar qualsevol mesura de seguretat.

MESURES DE SEGURETAT A IMPLANTAR A L'EMPRESA



Principals mesures de seguretat més necessàries i de fàcil adopció per minimitzar els riscos i fer l'empresa més resilient:

- Establir una política de **contrasenyes fortes i complexes**, úniques i unipersonals i que tinguin una caducitat raonable.
- **Actualitzar** els sistemes operatius i els programes.
- Gestionar correctament els **usuaris** i **permisos** d'accés als sistemes. És important donar de baixa els usuaris que abandonin l'empresa.
- Dotar tots els equips d'un **antivirus/*antimalware*** i implantar tallafocs a les xarxes i connexions a Internet.
- **Assegurar els mòbils de l'empresa:** que tinguin contrasenyes d'accés, que se'n puguin esborrar les dades remotament en cas de pèrdua o sostracció, antivirus...
- Fer **còpies de seguretat** de tots els arxius de manera freqüent. Assegurar la recuperació de forma efectiva.

- Mantenir un **inventari** de tots els equips de l'empresa i tenir a mà el *software* original.
- Fer **formació a l'equip** de l'empresa perquè tothom tingui consciència dels riscos, i saber detectar casos d'enginyeria social i intents d'estafa.
- Estar al dia en matèria de legislació de tot el que fa referència a **protecció de dades**.
- Fer periòdicament una **auditoria tècnica de seguretat** per avaluar riscos a la infraestructura tecnològica.

QUÈ HAN DE TENIR EN COMPTE LES PERSONES QUE TREBALLEN A L'EMPRESA?

Decàleg per compartir amb l'equip de l'empresa:

1. No s'han d'utilitzar les **contrasenyes** emprades a l'empresa en aplicacions d'ús personal.
2. No s'ha de **fer clic en enllaços sospitosos** i cal revisar bé si són legítims o no. Si cal, es pot escriure l'adreça on es vulgui anar a la barra del navegador.
3. Cal anar amb compte amb l'**ús del correu electrònic** i evitar els correus en cadena.
4. Cal **protegir la informació** en paper utilitzant armaris amb clau.
5. No s'ha de transportar la informació delicada en dispositius extraïbles. Si és indispensable, s'ha de **xifrar**.
6. Cal aprendre a **detectar els atacs** d'enginyeria social: si algú conegut se'ns dirigeix de manera inusual cal sospitar.
7. Cal **bloquejar la sessió** en l'equip quan s'abandona el lloc de treball.

8. No s'ha de modificar la **configuració del mòbil** d'empresa i no s'hi han d'instal·lar aplicacions no autoritzades.

9. **Cal evitar l'ús d'equips personals** per accedir a serveis de l'empresa. Si s'accedeix al correu corporatiu des de l'equip personal, no s'han de descarregar fitxers a l'equip.

10. Cal **destruir la informació delicada** en format paper. No n'hi ha prou en llençar-la a la paperera.

www.vnginnova.cat/ciberseguretat

VOLS SABER QUIN ÉS EL GRAU DE PROTECCIÓ DE LA TEVA EMPRESA?

Fes el test d'autoavaluació de Ciberseguretat a www.seguretat.info

Referències:

Informació elaborada parcialment a partir de les publicacions de l'Agència de Ciberseguretat de Catalunya i l'Instituto Nacional de Cibereguridad (Incibe) i ADQA.

Una campanya de ciberseguretat a les empreses impulsada per:

AJUNTAMENT DE Vilanova i la Geltrú

neàpolis

Oficina Municipal d'Empresa

Diputació Barcelona

FEGP Federació Empresarial del Gran Penedès

A·D·Q·A