10 errors freqüents de la seguretat digital de la teva empresa i com evitar-los.

Els **ciberdelinqüents també han tornat per Nadal**, llestos per portar carbó i programari maliciós a la seva empresa. A continuació, li **comptem 10 errors comuns** i com evitar-los aquests Nadal:

1. Facilitar les claus d' apoderats a personal administratiu no autoritzat.

Un dels errors més comuns, és donar accés a claus d' apoderats a personal administratiu. Potencialment, això pot ocasionar accessos no autoritzats.

Com actuar?

Per evitar qualsevol accés no autoritzat, les empreses han de comptar amb polítiques estrictes de control d' accés, emmagatzemant les claus de forma centralitzada i controlant-hi l' accés seguint el principi del mínim privilegi. A més, es recomana utilitzar autenticació multifactor (MFA) per a accessos sensibles, garantint que només persones autoritzades hi puguin accedir.

2. Compartir credencials per correu electrònic.

En compartir credencials per correu electrònic, com per exemple noms d'usuari i contrasenyes, s'exposa informació crítica a possibles atacs. Els atacants poden interceptar les comunicacions i obtenir visibilitat de tot el que hi compartim.

Com actuar?

Divideixi la informació, enviant el nom d'usuari i la contrasenya per diferents canals de comunicació (correu electrònic, trucada, SMS, etc.). Això redueix el risc que ambdues parts de les credencials siguin interceptades simultàniament per un ciberdelinqüent. Addicionalment, és convenient que la contrasenya proporcionada sigui temporal, havent de ser canviada pel destinatari immediatament després del primer ús. I, sempre que sigui possible, s' han d' aplicar tècniques de xifrat d' extrem a extrem en les comunicacions.

3. Emmagatzemar targetes de coordenades de forma insegura.

Guardar targetes de coordenades en mitjans no segurs, com fotografies al mòbil, o realitzant fotocòpies d'elles, augmenta el risc de robatori d'informació.

Com actuar?

Per minimitzar els riscos de revelació i l' ús indegut d' aquesta informació, eviti fer duplicats o extreure dades de la seva targeta de coordenades. Mantingui sempre aquestes targetes en un lloc segur i hi accedeixi només quan sigui absolutament necessari.

4. No verificar el compte bancari de proveïdors.

Pagar factures sense verificar regularment el compte corrent dels proveïdors, pot derivar en fraus com ara l'ingrés de pagaments en comptes bancaris fraudulentes/que pertanyin als atacants.

Com actuar?

Per evitar aquests fraus, és imprescindible que les empreses disposin de procediments de verificació obligatòria per a qualsevol canvi en el compte bancari de proveïdors, incloent-hi la confirmació directa de les dades amb una font confiable.

5. No confirmar canvis de compte bancari per telèfon.

És important confirmar telefònicament, amb l' interlocutor adequat, qualsevol canvi de compte bancari. No fer-ho pot permetre pagaments fraudulents, ja que els ciberdelinqüents podrien haver suplantat la identitat del destinatari legítim.

Com actuar?

Per protegir-se d'aquests atacs, les empreses han de tenir implantat un protocol de validació per múltiples canals (per exemple, trucades telefòniques, videoconferències) abans d'acceptar canvis en la informació de pagament.

6. Acceptar ordres per correu sense validació prèvia (Frau del CEO).

Executar ordres rebudes per correu sense verificar-les pot materialitzar possibles atacs de suplantació d' identitat, com ara phishing o spear phishing, on els atacants es fan passar per una persona o entitat legítima per enganyar la víctima.

Aquests atacants solen suplantar la identitat d'un alt càrrec, qui fent ús de la seva autoritat, trasllada urgència, rapidesa i discreció en l'operació sense fer preguntes i saltant-se els procediments habituals.

Com actuar?

Per evitar-ho, les organitzacions han de comptar amb una política de verificació per múltiples canals per a qualsevol ordre d' acció financera o de dades crítiques rebuda per correu, incloent mecanismes de report de qualsevol petició que intenti saltar-se les lleres establertes en aquesta política, independentment de qui sigui el peticionari.

7. Usar contrasenyes febles o repetides.

Les contrasenyes poc complexes faciliten l'èxit d'atacs de força bruta, que permet als ciberdelinqüents endevinar-les. A més, la repetició de contrasenyes permet als atacants accedir a múltiples comptes si una credencial és compromesa, exposant les empreses a bretxes de seguretat i robatori d'informació.

Com actuar?

Per mitigar aquests riscos, és essencial usar contrasenyes fortes i úniques per a cada compte. Les empreses han de disposar de polítiques robustes de control d'accés, preferiblement combinades amb autenticació multifactor (MFA) per agregar una capa addicional de seguretat.

8. No actualitzar programari ni aplicar pegats de seguretat.

No mantenir els sistemes actualitzats deixa les empreses vulnerables a atacs, ja que els ciberdelinqüents poden explotar fallades conegudes per realitzar atacs de diversa índole.

Com actuar?

És imprescindible que les empreses implementin polítiques de gestió d'actualitzacions que incloguin la instal·lació periòdica de la seguretat crítics. A més, és fonamental la realització de proves regulars de vulnerabilitats, amb l' objectiu d' identificar-les i esmenar-les com més aviat millor.

9. No realitzar còpies de seguretat regulars ni provar la seva restauració.

L' absència de backups, o no verificar les còpies de seguretat que es realitzen, exposa l' empresa a perdre informació crucial en cas d' un atac de ransomware o una fallada del sistema.

Com actuar?

Per evitar aquest risc, les empreses han de comptar amb polítiques i mecanismes de backup periòdics. Aquests backup s' han de verificar mitjançant proves periòdiques de restauració per assegurar la integritat de les dades recolzades.

10. No formar en seguretat digital els empleats.

El personal sense formació /conscienciació és més vulnerable a atacs de phishing i programari maliciós en mancar dels coneixements necessaris per identificar i evitar amenaces.

Com actuar?

Les organitzacions han de contemplar en els seus programes formatius la capacitació i conscienciació contínua en matèria de seguretat digital, amb accions que expliquin com reconèixer amenaces i emfatitzin la importància de la seva identificació.

A Bankinter treballem contínuament per la seva seguretat, si té dubtes davant de qualsevol situació, cridi al nostre **Servei d'Atenció al Frau: 900 81 00 62**.

A més, seguim la Directiva Europea PSD2 relativa als serveis de pagament, per això per a determinades operacions, li **demanarem una clau que enviarem per SMS al seu telèfon mòbil**.

Si desitja comprovar que el seu número de mòbil està correctament registrat, entri en **bankinter.com/empresas, i accedeixi a la seva Àrea de Gestió: Usuaris Perfils Signatura de Seguretat**.

bankinter.