Si të mbrohemi nga vjedhja e identitetit

Shumë njerëz nuk e bëjnë lidhjen midis emailit ose telefonatës dhe vjedhjes së identitetit. Por këto janë mënyra se si kriminelët kibernetikë dëmtojnë individët dhe organizatat.

Me anë të një emaili phishing ose telefonate mashtruese, kriminelët kibernetikë vjedhin informacione personale dhe financiare nga viktimat, të cilat më pas i përdorin për të marrë identitetet e tyre e më pas për ti dëmtuar keta njerëz dhe organizatat.

Ndikimet e vjedhjes së identitetit janë të rënda, si shkatërrimi i reputacionit i organizatës nga e cila kanë rrjedhur të dhënat, dëmtimi i të dhënave të punonjësit që instalon aksidentalisht ransomware dhe ekspozimi afatgjatë i të dhënave të klientëve / shitësve / partnerëve / kolegëve ndaj mashtrimeve financiare dhe personale.

Nuk ka kufizime se cfarë mund të bëjnë kriminelët kibernetikë me informacionin personal të vjedhur si, hapja e llogarive bankare, regjistrimi për kartat e kreditit deri tek aplikimi për punë në emër të viktimës.

Çfarë është vjedhja e identitetit?

Vjedhja e identitetit është akti i marrjes dhe përdorimit të informacionit personal të viktimës për të kryer aktivitete mashtruese në emër të atij personi. Me informacion të mjaftueshëm për viktimën e tyre, një kriminel merr identitetin e viktimës dhe kryen një sërë aktivitetesh mashtruese në emër të tij.

Ndërsa një viktimë dëmtohet personalisht nga vjedhja e identitetit, pasojat e sulmit kibernetik zakonisht nuk kufizohen vetëm në një person. Kriminelët kibernetikë zakonisht gjuajnë punonjësit në biznese, shkolla, insitucione qeveritare, spitale dhe institucione të tjera, duke shpresuar se një punonjës do të klikojë në një link të një emaili phishing për të aksesuar në bazat e të dhënave të informacionit personal dhe financiar.

Dëmi i bërë nga vjedhja e identitetit ka një efekt domino dhe dëmton të gjithë, duke shkaktuar trauma personale dhe emocionale për personin që aksidentalisht i jep akses kriminelëve kibernetikë, pasoja të rënda për njerëzit të cilëve u është vjedhur informacioni personal dhe dëmtimi i reputacionit të organizatës.

Përvec vjedhjes së informacionit personal dhe financiar të punonjësve, klientëve, investitorëve dhe partnerëve të palëve të treta, vjedhja e identitetit dhe rjedhja e të dhënave, sjellin dëme edhe në tre mënyra kryesore:

- Humbje financiare: kjo përfshin kostot e rikuperimit nga një rrjedhje e të dhënave, kryerjen e pagesave të ransomware, kompensimin e viktimave, rritjen e primeve të sigurimit, rindërtimin e rrjeteve kompjuterike dhe infrastrukturës teknike, mbylljen e biznesit.

- Reputacioni dhe besimi: është shumë e vështirë të rindërtohet besimi brenda dhe jashtë organizatës kur një sulm kibernetik shkakton vjedhje identiteti. Rindërtimi i besimit me klientët, partnerët dhe mediat kushton, kërkon shumë kohë dhe është shumë i vështirë.

- Ndikimi në biznes: nëse vjedhja e identitetit ka ndodhur në një shkollë, organizatë e kujdesit shëndetësor, korporatë e madhe ose departament qeveritar – ndikimet e biznesit janë të gjata. Kjo ndodh pasi ka humbje të pronës konfidenciale dhe intelektuale, ka kosto të lartë të rindërtimit të biznesit, ka kosto ligjore dhe humbje të mundësive të ardhshme të biznesit.

Për shkak se shumë njerëz dhe punonjës nuk janë në dijeni se si ndikon rrjedhja e të dhënave dhe sulmet kibernetike në botën reale, ata duhet të informohen se çfarë do të thotë vjedhja e identitetit për ta në nivel personal.

Vjedhja e identitetit mundëson që krimineli kibernetik të përdorë identitetin e viktimës për:

- Akumulimin e tarifave të kartës së kreditit.
- Marrja e një kredie të re.
- Transferimin e shumave monetare nga llogaria e viktimës.
- Nënshkrimi i një kontratë qiraje në emër të viktimës.
- Marrja e përfitimeve të shumave monetare që qeveria i detyrohet viktimës.
- Marrja e dokumenteve identifikuese ose të udhëtimit.

Vjedhja e identitetit kryhet nga kriminelët kibernetikë duke perdorur këto metoda kryesore të sulmeve kibernetike:

- Inxhinierinë sociale duke dërguar email ose mesazh telefonik.
- Malware – si instalimi në rrjet i softuerit spyware ose keyloggers.
- Kërkimi në faqet e mediave sociale të viktimës për informacione personale, adresa emaili, për njohje midis punonjësve, konferenca më të fundit të kryera prej tij, promovime, etj.
- Hakimi i kompjuterit dhe bazave të të dhënave përmes një sërë taktikash.
- Përgjimet e bisedave telefonike në vendet publike të punonjesve, si telefonatat në hollin e godinës së zyrës, në autobus etj.
- Marrja e dokumenteve nga kutitë postare, nga koshat e riciklimit ose koshat e plehrave dhe përdorimi i këtij informacioni për të kryer vjedhje identiteti ose sulme shtesë kibernetike, si peshkim i targetuar (spear phishing) ose kompromentim i emailave të biznesi (business email compromise).
- Krijimi i profileve të rreme në media sociale duke bindur punonjësit që të bëjnë kujdes ndaj një telefonuesi ose dërguesi emaili i panjohur për të krijuar përshtypjen tek viktima se personi është i besueshëm.

Për të mbrojtur veten, organizatën dhe punonjësit tuaj nga një incident i vjedhjes së identitetit, duhen ndjekur këto praktika më të mira të sigurisë kibernetike:

1. Përdorimi i sulmeve phishing të stimuluar për të kontrolluar ndërgjegjësimin e punonjësve rreth sulmeve phishing dhe për të matur efektivitetin e trajnimeve dhe fushatave të ndërgjegjësimit për sigurinë kibernetike.
2. Përdorimi i buletineve dhe fushatave të tjera informuese për të rritur ndërgjegjësimin e punonjësve për metodat dhe dëmet e vjedhjes së identitetit.
3. Punonjësit duhen të përdorin me kujdes faqet e rrjeteve sociale si LinkedIn, Twitter, Instagram dhe Facebook. Kriminelët kibernetikë përdorin informacionin e marrë nga këto faqe për të dërguar emaile bindëse ose për të bërë telefonata mashtruese.
4. Punonjësit duhet të marrin pjesë ose të kenë akses në materialet e trajnimeve më të fundit të ndërgjegjësimit për sigurinë kibernetike mbi tema të tilla si inxhinieria sociale, vjedhja e identitetit, vishing dhe smishing.
5. Punonjësit duhet të informohen rreth politikave të kompanisë për punën në distancë, si siguria e punës nga shtëpia dhe sigurinë e pajisjeve (BYOD-Bring Your Own Device).
6. Vendosja e politikave të forta për krijimin e fjalëkalimeve nga punonjësit, të cilët duhen detyruar ti përditësojnë rregullisht ato.
7. Nuk duhet dhënë informacione konfidenciale personale ose të organizatës përmes telefonit ose duke postuar në një faqe interneti. Gjithmonë duhet verifikuar legjitimiteti i organizatës dhe personit që kërkon informacionin. Kur ka dyshime rreth kërkesës, duhet biseduar me menaxherin e kompanisë.
8. Kur plotësohen formularët dhe jepen informacione në internet, duhet që URL-ja e uebsajtit të përdor https:// dhe të ketë ikonën e drynit në fushën e URL-së. Kjo tregon se faqja e internetit është e sigurt.
9. Nuk duhet dhënë detaje personale si data e lindjes, numri i sigurimeve shoqërore, adresa postare ose informacione të tjera private, njerëzve që ju telefonojnë, ju dërgojnë mesazhe ose email.
10. Nuk duhet të shkruhet PIN-i ose fjalëkalimet. Ato duhet te mësohen përmendësh ose të përdoret një mjet fjalëkalimesh për ti ruajtur ato në mënyrë të sigurt.
11. Duhen asgjësuar në mënyrë të sigurt dokumentet që përmbajnë informacione personale ose konfidenciale të kompanisë kur ato nuk janë më të nevojshme.
12. Informacione personale dhe konfidenciale duhet të komunikohen me kolegët duke përdorur metoda të sigurta, si emaili i koduar.
13. Duhet verifikuar identiteti i një telefonuesi përpara se të jepet informacioni në telefon. Kjo përfshin edhe telefonuesin që thotë se është klient, shitës ose partner i palës së tretë.
14. Duhet treguar kujdes me njerëzit që identifikohen si anketues ose përfaqësojnë organizata qeveritare që bëjnë thirrje për të mbledhur informacion për qëllime statistikore ose kërkimore. Këta njerëz nuk duhet t'ju kërkojnë informacione të tilla si data e lindjes, adresa postare, paga, diploma akademike ose mbiemri i vajzërisë së nënës.

Nëse dyshoni se i keni dhënë aksidentalisht informacion një krimineli kibernetik, kontaktoni menjëherë ekipin tuaj të IT ose të kërkoni ndihmë. Sa më shpejt të njoftoni, aq më shpejt mund të reagohet dhe të kufizohen ndikimet negative.