NXHINIERIA SOCIALE, LLOJET E SULMEVE DHE PARANDALIMI

Inxhinieria Sociale është veprimi i manipulimit të njerëzve për të dhënë informacion konfidencial ose të ndjeshëm. Kjo mund të bëhet me telefon, email ose nëpërmjet kontaktit ballë për ballë. Është metoda më e vjetër që përdoret ende sot për mbledhjen e informacionit. Inxhinieria sociale përdoret shpesh në emailat spam dhe phishing.

LLOJET E SULMEVE TË INXHINIERISË SOCIALE:

1.Phishing: Phishing është metoda e marrjes së fjalëkalimeve, të dhënave të llogarisë së bankës ose të dhënave të kartës së kreditit duke u maskuar si një element i besueshëm në komunikimet elektronike si emaili ose biseda elektronike (chat). Fjala 'phish' përkthehet 'peshk' e cila është zgjedhur pasi metoda përdor mashtrimin e viktimës për të mbledhur informacion e dëshiruar njësoj si karremi i peshkimit imiton lëvizjen e krijesave që notojnë për të mashtruar peshkun.

Email-et "të krijuara me kujdes dhe të personalizuara" duken sikur vijnë nga kompani të ligjshme, duke informuar punonjësit se llogaria e tyre bankare është kompromet uar ose se duhet të përditësojë informacionin e tyre. Viktimat sapo të klikojnë në linkun e dërguar në email, drejtohen tek një faqe interneti mashtruese e cila është një faqe sulmi ku mblidhen të dhënat e tyre.

2.Vishing: Vishing është shkurtim për “peshkim i zërit”, phishing telefonik duke përdorur sistemin VoIP (Voice Over IP). Vektori i sulmit për këtë lloj inxhinierie sociale është i njëjtë me phishing, vecse sulmi bëhet përmes telefonit. Një sulmues bën një telefonatë jo të vërtetë VoIP drejt objektivit dhe paraqitet si një organizatë që viktima do t'i besonte.

3. Spear phishing: Spear phishing ngjason me sulmet e phishing me ndryshimin që sulmuesit shpesh përdorin spear-phishing për të anashkaluar muret e zjarrit (firewalls) dhe masat e tjera të sigurisë pasi emaili vjen nga dikush që është në domenin e kompanisë.

4. Shkarkimi i kredencialeve (Credential Dumping): Shkarkimi i kredencialeve ndodh kur sulmuesi mbledh informacione tëlogimit ose kredencialet e bazës së të dhënave nga sisteme, serverë ose faqe interneti të kompromet uara. Sulmuesi më pas e përdor këtë informacion për të hyrë në sisteme të tjera, potencialisht më të sigurta.

5. Baiting: Ndodh kur sulmuesit lënë pajisjen USB ose CD që përmbajnë softuer dashakeq në një zonë ku ata e dinë se do të jenë punonjësit. Ata shpresojnë se dikush do të marrë një nga këto pajisje në shtëpi dhe do ta futë në kompjuterin e tyre, e cila më pas mund të kompromentohet.

6. Smishing: Smishing është kombinim i phishing dhe mesazheve SMS me anë të celularit. Sulmuesit dërgojnë mesazhe tekst me linke për përdoruesit te cilët mund të mashtrohen nëse klikojnë në link dhe japin informacione personale, duke menduar se SMS vjen nga një bankë ose ofrues shërbimi i besueshëm.

7. Spear phishing nëpërmjet rrjeteve sociale: Ky lloj phishing përdor shërbimet e rrjeteve sociale për të përhapur malware, për të vjedhur informacionin personal të përdoruesve dhe për të fituar

akses në llogaritë e tyre. Sulmuesit shpesh përpiqen të bëjnë miq persona nga e njëjta organizatë ose grup rrjeti për t'i shtuar ata në rrjete e tyre sociale për të rritur besueshmërinë e tyre.

8. Waterhole: Në këtë lloj sulmi, një haker keqdashës kompromenton një faqe web ose pajisje, me qëllim që sulmuesit e tjerë të përfitojnë prej tij. Për shembull, një haker dashakeq mund të lërë një kompjuter me dobësi sigurie të hapur për publikun, duke shpresuar se një haker tjetër do t'i shfrytëzojë ato dobësi.

9. Inxhinieri sociale për platformat e celularëve: Në këtë sulm të inxhinierisë sociale, hakeri, hyn në telefonin inteligjent të një përdoruesi për të kërkuar informacione sensitive. Një mashtrues dërgon mesazhe, duke kërkuar kredencialet tuaja të loginit ose informacionin e kartës së kreditit në mënyrë që "të mund të përditësojnë të dhënat e faturimit". Nëse ju i jepni të dhenat, ata do të kenë akses në informacionin tuaj personal.

10. Scareware: Ndodh kur një sulmues përpiqet tju mashtrojë që të mendoni se kompjuteri ose celulari juaj ka një virus të instaluar. Ata e bëjnë këtë duke instaluar një program të rremë antivirus e cila shfaqet në ekranin e kompjuterit ose celularit dhe pretendon në mënyrë të rreme se ka kërcënime të pranishme. Në këtë mënyrë përdoruesi detyrohet të paguajë për programin antivirus të rremë qe t'i heqë këto viruse. Më pas sulmuesit përdorin informacionin e kartës suaj të kreditit për të bërë blerje të paautorizuara.

11. Tailgating and piggybacking: Një sulmues përdor dikë tjetër për të hyr në një zonë të kufizuar, si p.sh. ndjekja nga pas derës të punonjësve të organizatës, pasi ata e dinë që ajo po mbahet e hapur për dikë. Ky sulm përdoret gjithashtu nga sulmuesit që shpresojnë të përdorin kredencialete e tua të organizatës.

12. Kompensim (Quid Pro Quo): Përdoret kur një sulmues ofron të bëjë diçka për ju në këmbim të bashkëpunimit tuaj ose heshtjes për veprimet e tyre të paligjshme. Për shembull, sulmuesit mund të përdorin Quid Pro Quo duke ofruar përmirësimin e sistemit tuaj kompjuterik nëse i lejoni atij qasje të përkohshme në të.

13. Gjuetia e balenave (Whaling): Gjuetia e balenave është një lloj specifik sulmi phishing që synon punonjësit drejtues të rangut të lartë të organizatës. Sulmuesit monitorojnë mediat sociale dhe emailet për të dhëna mbi udhëheqjen e organizatës dhe me pas u dërgojnë atyre mesazhe specifike me linke ose bashkëngjitje (attachments) të cilat mund të rrezikojnë sigurinë e tyre.

14. Brute Forcing: I njohur gjithashtu si "password cracking", i cili ndodh kur një sulmues përdor një program që hamendëson me shpejtësi cdo lloj fjalëkalimi për të hyrë në llogarinë ose sistemin e një përdoruesi.

15. Pharming: Ky sulm përfshin hakerët që modifikojnë të dhënat DNS për faqet e internetit te njohura dhe te ligjshme, si faqet e bankave, faqet e blerjeve online, në mënyrë që përdoruesit kur përpiqet të aksesojnë faqen e vërtetë, dërgohet në versione të rreme (dhe shpesh me qëllim të keq) të atyre faqeve. Në këtë mënyrë, kur perdoruesi shkruan emrin e përdoruesit dhe fjalëkalimin ose informacionin e kartës së kreditit në një faqe interneti të rreme që duket tamam si origjinali, hakerët fitojnë akses në të dhënat e tyre.

16. Përgjimi: Një haker keqdashës mund të lidhet në një kabllo telefonike për të dëgjuar bisedat ose për të vjedhur informacion nga një rrjet kompjuterik.

KËSHILLA PËR TË PARANDALUAR SULMET E INXHINIERISË SOCIALE:

1. Shmangni klikimin e bashkëngjitjeve (attachments) nga burime të panjohura. Edhe nëse emaili vjen nga dikush të cilit i besoni, jini të kujdesshëm, pasi hakerët mund të mashtrojnë edhe adresat e tyre të emailit.
2. Nëse një faqe interneti duket e dyshimtë ose nuk duket e ligjshme, shmangni vendosjen e informacionit tuaj personal ose financiar dhe kontaktoni administratorin tuaj të TI-së për detaje të mëtejshme rreth faqes.
3. Mos jepni asnjë informacion personal përmes telefonit nëse nuk e keni nisur kontaktin me kompanine që njihet tashmë. Është më mirë të komunikoni me ta përmes një burimi zyrtar si faqja e tyre e internetit.
4. Kur është e mundur, kur identifikoheni në faqet e internetit ose aplikacionet, përdorni autentikimin me dy faktorë, në mënyrë që nëse fjalëkalimi juaj komprometohet, sulmuesit nuk mund të hyjnë në llogarinë tuaj pa pasur akses fizik në smartfonin tuaj ose në një pajisje tjetër që përdoret si "çelës" i llogarisë tuaj.
5. Kur zhvendoseni në një apartament të ri, ndryshoni të gjitha fjalëkalimet tuaja dhe mbyllni çdo llogari ekzistuese që lidhen me adresën e mëparshme si media sociale, pasqyra financiare, email, etj, në mënyrë që të mos ekspozoheni ndaj rrezikut personal.
6. Kur blini ose shisni artikuj në mediat sociale, gjithmonë merreni produktin në një vend publik me shumë njerëz përreth dhe mos shkoni kurrë vetëm.

MOS BINI VIKTIMË:

Fatkeqësisht, përdoruesit dhe organizatat janë shpesh objektiva të sulmeve të inxhinierisë sociale dhe shumica e njerëzve nuk i njohin ato, ose nuk dinë si të mbrohen ndaj tyre.

Për t'u mbrojtur nga këto kërcënime, si punonjësit ashtu edhe pronarët e bizneseve duhet të familjarizohen me strategjitë e përbashkëta të inxhinierisë sociale. Për më tepër, organizatat duhet të zbatojnë politika që u kërkojnë punonjësve të tyre të kryejnë trajnime për ndërgjegjësimin e sigurisë, për të zvogëluar rrezikun për t'u bërë viktima të mashtrimeve të inxhinierisë sociale.