Det månedlige nyhedsbrev om IT-sikkerhed til dig

Personaliseret svindel

Oversigt

IT-kriminelle fortsætter med at komme på nye og kreative måder at narre folk på. En ny type svindel er ved at blive populær - den personaliseret svindel (”personalized scams”). IT-kriminelle finder eller køber information om millioner af mennesker, og bruger så disse oplysninger til at personalisere deres angreb. Nedenfor viser vi dig, hvordan disse svindlere arbejder og går igennem et eksempel. Jo mere du ved om denne type svindel, desto lettere er det for dig at få øje på og stoppe det.

Hvordan virker det?

Svindel ved hjælp af e-mail eller telefonopkald er ikke nyt, IT-kriminelle har forsøgt at narre folk i årevis. Eksempler herpå er “Du vandt lotteriet” eller den berygtede ”nigerianske prins”-svindel. Men i disse traditionelle eksempler på svindel ved de IT-kriminelle ikke, hvem de rammer. De skaber simpelthen en generisk besked og sender den ud til millioner af mennesker. Fordi disse svindelnumre er så generelle, er de normalt let at få øje på. En personaliseret svindel er anderledes, IT-kriminelle undersøger først deres påtænkte offer og opretter en tilpasset besked til hvert offer. De gør dette ved at finde eller købe en database over folks navne, adgangskoder, telefonnumre eller andre detaljer. Denne type information er let tilgængelig på grund af alle de websteder, der er blevet hacket. Det er også almindeligt tilgængeligt på sociale medier og i offentligt tilgængelige databaser. De kriminelle retter derefter deres angreb mod alle, de har oplysninger om.

En almindeligt trick, som de IT-kriminelle bruger, er frygt eller afpresning for at lokke dig til at betale dem penge. Et angreb kunne eksempelvis være: De IT-kriminelle finder eller køber oplysninger om folks logins og adgangskoder fra hackede hjemmesider. De finder dine kontooplysninger inkluderet i denne database og sender dig (og alle andre i databasen) en e-mail med nogle personlige oplysninger om dig, herunder det originale kodeord, du brugte på den hackede hjemmeside. Den IT-kriminelle henviser til dit kodeord som “bevis” for at hacket din egen computer eller enhed, hvilket selvfølgelig ikke er sandt. Den kriminelle hævder derefter, at mens de hackede din computer, fik de også beviser på at du ser pornografi online. E-mailen truer så med, at hvis du ikke betaler deres pris, deler de beviserne på dine pinlige onlineaktiviteter med dine familie og venner.

I en situation som denne har den IT-kriminelle næsten aldrig hacket dit system. De ved ikke engang, hvem du er, eller hvilke hjemmesider du har besøgt. Svindleren forsøger simpelthen at bruge de få personlige oplysninger, de har om dig, til at skræmme

dig til at tro, at de har hacket din computer eller enhed, og at narre dig til at betale dem penge. Husk, de kriminelle kan bruge de samme teknikker til telefonsvindel.

Hvad skal jeg gøre?

Du skal vide, at e-mails eller telefonopkald som disse er et fupnummer. Det er naturligt at føle sig bange, når nogen har personlige oplysninger om dig. Men husk, at afsenderen lyver. Angrebet er en del af et automatiseret masseangreb, ikke et forsøg på at ramme dig direkte. Det er meget lettere for IT-kriminelle i dag at finde eller købe personlige oplysninger, så forvent mere personaliseret svindel som dette i fremtiden. Nogle elementer at være på udkig efter.

⚠

- **Når du modtager en meget presserende e-mail, besked eller telefonopkald, skal du være meget mistænkelig. Hvis nogen bruger følelsen af frygt eller at det haster, er det fordi de forsøger at skynde dig til at begå en fejltagelse.**
- **Når en person kræver betaling i BitCoin, gavekort eller anden valuta der ikke kan spores**
- **Når du får en mistænkelig e-mail, skal du søge på Google for at se, om andre har rapporteret et lignende angreb.**

I sidste ende er sund fornuft dit bedste forsvar. Vi anbefaler dog også, at du altid bruger et unikt, langt password til hvert af dine online-konti. Kan du ikke huske alle dine adgangskoder? Brug en adgangskodeadministrator. Desuden skal du aktivere to-trins bekræftelse, hvor det er muligt.

WelcomeSecurity samarbejder med netop din virksomhed om at identificere de IT sikkerhedsmæssige risici, som truer din virksomhed. Ved at analysere og teste jeres processer, teknologi og ikke mindst jeres medarbejder vil vi fastslå de mest effektive måder at minimere disse risici. Du kan finde os på https://www.welcomesecurity.net.

Gæsteredaktør

Lenny Zeltser *er en gammel kending indenfor IT-sikkerhed. Han bygger anti-malware løsninger på Minerva Labs og underviser i IT-sikkerhed på SANS Institute. Han har også leveret sikkerhedstjenester og rådgivning til kunder. Følg ham på* zeltser.com/blog*) og på Twitter* @lennyzeltser*.*

Hvis du vil vide mere

Social Engineering:	https://www.sans.org/u/MUU
Stop That Phish:	https://www.sans.org/u/MUZ
Search Yourself Online:	https://www.sans.org/u/MV4
Password Manager:	https://www.sans.org/u/MV9