Kuukausittainen uutiskirje tietoturvatietoisuuteen liittyvistä aiheista

OUCH!

Tässä numerossa…

- **Mitä sosiaalinen hakkerointi on?**
- **Sosiaalisen hakkeroinnin havainnointi ja estäminen**

Sosiaalinen hakkerointi

Yleiskatsaus

Yleinen harhaluulo kyberhyökkäyksistä on se, että niissä käytetään aina uusimpia tekniikoita ja viimeisintä teknologiaa. Tämä ei ole totta, vaan kyberrikolliset ovat todenneet, että yleensä yksinkertaisin tapa varastaa tietoja, hakkeroida tilisi tai saastuttaa laitteesi on huijata sinut tekemään virhe. Tässä uutiskirjeessä kerromme mitä sosiaalinen hakkerointi on, miten se toimii ja mitä sinä voit tehdä suojataksesi itseäsi.

Vierastoimittaja
James Lyne (**@jameslyne**) on sertifioitu SANS-kouluttaja ja toimii globaalina tutkimusjohtajana Sophos-nimisessä yrityksessä. Hän purkaa ja takaisinmallentaa viimeisimpiä ja suurimpia kyberrikollisten luomuksia. Hän on kirjoittanut materiaalit SANS:n “Metasploit (SEC580)” ja “Social Engineering (SEC567)”-kursseille.

Mitä sosiaalinen hakkerointi on?

Sosiaalinen hakkerointi viittaa psykologiseen hyökkäykseen, jossa hyökkääjä huijaa sinut tekemään jotain mitä sinun ei pitäisi tehdä. Sosiaalisen Hakkeroinnin konsepti ei sinänsä ole uusi, ihmisiä on huijattu jo tuhansia vuosia, mutta ennen tietokoneita samoja toimintatapoja käytettiin muunlaisiin huijauksiin. Suurin ero digitaaliseen maailmaan on se, että et näe huijaria, huijari voi tekeytyä keneksi vaan ja huijauksen voi helposti kohdistaa tuhansiin uhreihin samanaikaisesti. Lisäksi sosiaalisen hakkeroinnin avulla voidaan ohittaa monia perinteisiä suojamekanismeja ja teknologioita. Alla on kaksi oikeaa esimerkkiä jotka selittävät sosiaalisen hakkeroinnin periaatteita. Saat puhelun palveluntarjoajasi tai Microsoftin IT-tuesta ja soittaja kertoo, että koneesi lähettelee dataa internettiin ja hän uskoo, että koneesi on saastunut. Henkilöä on pyydetty auttamaan sinua ja korjaamaan saastunut koneesi.

Tämän jälkeen henkilö käyttää monimutkia IT-termejä ja pyytää sinua tekemään erinäisiä monimutkaisia asioita koneellesi näyttääkseen sinulle, että koneesi olisi saastunut. Sinua saatetaan pyytää löytämään tiettyjä tiedostoja koneeltasi ja kun löydät ne, soittaja vakuuttaa, että kyseinen tiedosto liittyy haittaohjelmaan, vaikka tosiasiassa kyse on normaalista käyttöjärjestelmään kuuluvasta tiedostosta. Kun uskot, että koneesi on saastunut, soittaja pyytää sinua asentamaan etähallintasovelluksen, jotta hän pystyy korjaamaan koneesi. Asennettu sovellus on tosiasiassa haittaohjelma ja kun asennat sen koneellesi, hyökkääjä

Sosiaalinen hakkerointi

saa vapaan pääsyn siihen. Tämän jälkeen hyökkääjä voi tehdä koneella mitä haluaa.

Toisessa esimerkissä kerrotaan toimitusjohtajahuijauksesta, joka on hyvin yleinen yrityksiin kohdistuva huijaustyyppi. Kyberhyökkääjä tutkii yrityksesi taustat ja selvittää esimiehesi tai jonkun yrityksen johtajan yhteystiedot. Tämän jälkeen hyökkääjä lähettää sinulle tämän henkilön nimissä sähköpostin jossa hän pyytää sinulta nopeita toimia, kun lähettää rahaa tai luottamuksellista tietoa. Usein tämänlaisissa sähköposteissa pyydetään kiireellisesti ohittamaan joitakin yrityksen suojausmekanismeja, kuten lähettää sähköpostia muuhun kuin yrityksen viralliseen osoitteeseen. Tämänlaiset hyökkäykset ovat erityisen vaarallisia, koska hyökkääjät yleensä tekevät erittäin paljon esiselvitystä ja tietoturvateknologiat, kuten antivirus-sovellukset eivät pysty reagoimaan näihin, koska hyökkäykseen ei sisälly mitään haittaohjelmia tai haitallisia linkkejä.

Terve järki on paras keino tunnistaa ja suojautua sosiaalista hakkerointia vastaan.

On hyvä muistaa, että sosiaalinen hakkerointi ei rajoitu puhelimeen tai sähköpostiin, ne voivat tapahtua myös muiden välineiden avulla, kuten tekstiviestillä, sosiaalisessa mediassa tai jopa kasvotusten. Tärkeintä on ymmärtää hälytysmerkit, koska sinä itse olet paras keino suojautumaan tallaisilta hyökkäyksiltä.

Sosiaalisen hakkeroinnin havainnointi ja estäminen

Onneksi sosiaalisen hakkeroinnin havainnointi ja estäminen on helpompaa kuin yleisesti oletetaan - terve järki on tehokkain keino. Jos joku vaikuttaa epäilyttävältä tai ei tunnu täysin oikealta, kyse saattaa olla hyökkäyksestä. Sosiaalisen hakkeroinnin yleisimmät merkit ovat:

- Joku yrittää luoda kiireyden tai tärkeyden tunnetta, tällä tavalla yritetään saada sinut tekemään virhe ajattelematta asiaa.
- Joku pyytää sinulta tietoja jotka heidän pitäisi tietää tai joita heidän ei pitäisi saada tietää, kuten luottokorttisi numero.
- Joku kysyy salasanaasi, mikään asiallinen taho ei tule koskaan kysymään salasanaasi missään yhteydessä.

Sosiaalinen hakkerointi

- Joku painostaa sinua ohittamaan tai olemaan välittämättä jostakin yrityksesi turvallisuussäännöstä tai ohjeesta, joita sinun oletetaan noudattavan.
- Jokin asia vaikuttaa olevan liian hyvää ollakseen totta. Voit saada esimerkiksi viestin jossa kerrotaan sinun voittaneen arvonnassa, vaikka et ole osallistunut.
- Saat oudon sähköpostin tutultasi tai kollegalta, jossa viestin sävy tai joku muu ei vaikuta tutulta tai normaalilta. Kyberhyökkääjä on saattanut murtautua heidän tililleen ja käyttää sitä sinua vastaan. Näissä tapauksissa kannattaa olla yhteydessä kyseiseen henkilöön jotakin muuta kautta, soittamalla tai kasvotusten.

Jos epäilet jonkun yrittävän huijata sinua, älä jatka kommunikointia kyseisen henkilön kanssa. Jos hyökkäys tapahtuu työympäristössä, ilmoita siitä esimiehellesi tai yrityksesi turvallisuushenkilöstölle. Muista, että terve järki on yleensä paras keino puolustautua.

LUE LISÄÄ

Liity kuukausittaisen OUCH! tietoturvatietoisuus-uutiskirjeen postituslistalle, lue OUCH! arkistoja ja tutustu SANS-järjestön muihin tietoturvatietoisuuteen liittyviin ratkaisuihin osoitteessa securingthehuman.sans.org/ouch/archives.

Uutiskirjeen kääntäjä Kirill Filatov (KTM) on GIAC-sertifioitu tietoturvaa rakastava IT-johtaja. Kirill turvaa tällä hetkellä Elisa Appelsiinin liiketoimintaa vastaamalla niin yrityksen omasta kuin asiakkaiden tietoturvasta.

Lähteet

Kalastelu:	https://securingthehuman.sans.org/ouch/2015#december2015
Toimitusjohtajahuijaus:	https://securingthehuman.sans.org/ouch/2016#july2016
Kiristyshaittaohjelmat:	https://securingthehuman.sans.org/ouch/2016#august2016
OUCH arkistot:	https://securingthehuman.sans.org/ouch/archives

Lisenssi