Salasanan käyttö

Johdanto

Tässä mikroharjoituksessa keskitytään salasanojen käyttöön. Kyseessä on lyhyt ja napakka harjoitus, jossa aiheeseen tutustutaan interaktiivisten aktiviteettien avulla, käsitellen yleisiä salasanojen käyttötapoja, kuinka hyökkääjät löytävät salasanasi ja mitä voit tehdä vähentääksesi riskiä salasanojesi paljastumiselle.

Kesto

Harjoitus kestää noin 15–30 minuuttia.

Osallistujat

Mukana voi olla niin suuri tai pieni osa henkilökunnasta kuin haluat, eikä kenenkään harjoitukseen osallistuvan tarvitse olla tietoturva-asiantuntija. Jos osallistujia on enemmän kuin yksi, suosittelemme nimeämään harjoituksen johtajan, joka johtaa harjoitusta ja pitää keskustellut oikeilla raiteilla.

Mitä osallistujilta odotetaan?

Harjoituksen tavoitteena on keskustella, oppia ja pohtia aihetta. Sinun ei tarvitse olla tietoturva-asiantuntija; kyseessä ei ole testi. Sen sijaan pyrimme mahdollistamaan yhteistoiminnalliset keskustelut, jotka syventävät tietämystäsi ja auttavat sinua tunnistamaan parannuskohteita.

Tilanne

Kun salasanojen määrä ja monimutkaisuus kasvavat, se asettaa käyttäjille kohtuuttomia vaatimuksia. Käyttäjät kehittävät väistämättä omia tapojaan navigoida tässä "salasanarallissa". Näihin keinoihin kuuluu:

- Sama salasana käytössä useissa eri järjestelmissä
- Helppojen ja arvattavien salasanojen luominen
- Salasanojen kirjaaminen ylös helposti löydettäviin paikkoihin.

Nämä tunnetut selviytymisstrategiat tarjoavat mahdollisuuksia hyökkääjille, jotka voivat hyödyntää niitä ja jättää henkilöstön ja organisaation

haavoittuvaisiksi. Tässä lyhyessä harjoituksessa tarkastellaan salasanojen hallintaa, hyökkääjien salasanojen löytöstrategioita ja keinoja vähentää riskiä joutua hyökkäyksen kohteeksi.

Keskustelu

Kysymys 1/4

Mikä on Suomessa eniten hakkeroitu salasana?

salasana
123456
perkele
qwerty

Vastaus:

Haveibeenpwned-sivuston (https://haveibeenpwned.com/) mukaan salasana "123456" on löydetty 23 miljoonaa kertaa. "qwerty" löytyi lähes 4 miljoona kertaa, ”salasana” lähes 19 000 kertaa ja "perkele" lähes 13 000 kertaa. "123456789" ja "salasana123" löytyvät myös tietovuodoista. Haveibeenpwned-sivustolla voit asettaa hälytyksen sähköpostiosoitteellesi. Kun sähköpostiosoitteesi löytyy tietovuodosta, saat siitä ilmoituksen. Voit myös testata salasanasi nähdäksesi, ovatko ne olleet jo osana tietovuotoa. Sivustoa ylläpitävät vapaehtoiset ja se on luotettava.

Kysymys 2/4

Mikä on Suomessa eniten hakkeroitu salasana, joka perustuu kuvitteellisen hahmon nimeen?

nallepuh
akuankka
dragon
tiikeri

Vastaus

Salasana "dragon" on havaittu tietovuodoissa lähes 1,5 miljoona kertaa. Nämä vaarantuneet salasanat on saatu Suomessa tietovuodoista, jotka ovat jo julkisesti saatavilla, kun ne on myyty ja jaettu hakkerien toimesta. Jos salasanasi on tässä listassa (https://dawn.fi/uutiset/2021/11/26/200-yleisinta-salasanaa-suomi-2021), sinun tulisi vaihtaa se välittömästi.

Kysymys 3/4

Pohdi, miten rikolliset pääsisivät käsiksi sinun salasanaasi.

Vastaus

Kalastelu (Phishing): Rikolliset lähettävät huijaavia sähköposteja tai viestejä, jotka näyttävät olevan luotettavista lähteistä. Näissä viesteissä pyydetään usein käyttäjiä paljastamaan salasanojaan tai kirjautumaan väärennettyihin verkkosivustoihin.

Sosiaalinen manipulointi (Social Engineering): Rikolliset käyttävät psykologisia manipulointikeinoja saadakseen käyttäjän paljastamaan salasanan. Tämä voi tapahtua esimerkiksi valepuheluiden, valheellisten tarinoiden tai muun manipuloinnin avulla.

Yleiset ja ilmeiset salasanat: Käyttäjät saattavat käyttää helposti arvattavia salasanoja, kuten "salasana" tai "123456", jotka voivat murtua alle sekunnissa.

Salasanan uudelleenkäyttö: Käyttäjät saattavat käyttää samaa salasanaa useissa eri palveluissa. Jos yksi tili on hakkeroitu, rikolliset voivat käyttää samaa salasanaa päästäkseen muihin tileihin.

Tietovuodot: Kun verkkopalvelu tai organisaatio joutuu tietomurron kohteeksi, salasanoja voi vuotaa julkisuuteen. Rikolliset voivat käyttää näitä vuotaneita salasanoja yrittäessään kirjautua muihin tileihin.

Brute Force -hyökkäys: Rikolliset käyttävät ohjelmistoja, jotka yrittävät automaattisesti arvata salasanan yrittämällä kaikkia mahdollisia kombinaatioita, kunnes oikea salasana löytyy.

Keylogging: Haittaohjelmat tallentavat kaikki näppäimistöllä kirjoitetut merkit, mukaan lukien salasanat, ja lähettävät ne hakkerin hallinnoimaan palvelimeen.

Kysymys 4/4

Valitse paras salasana alla olevasta listasta.

S4l4s4n4!
Leijonat123
Akuankka!!!
3PunainenAurinkoApina27!

Hyvä tapa luoda vahva ja helposti muistettava salasana on käyttää kolmea satunnaista sanaa. Vahva salasana sisältää:

- Pieniä kirjaimia
- Isoja kirjaimia
- Erikoismerkkejä
- Numeroita

Välilyönti on erikoismerkki. Aika moni palvelu sallii sen käytön, eli voit käyttää tavallista lausetta salasanana. On suositeltavaa, ettet koskaan käytä seuraavia henkilökohtaisia tietoja salasanassasi:

- Perheenjäsenten nimiä
- Lemmikkien nimiä
- Syntymäpaikka, -päivä
- Mökin paikkakunta tai suosikki lomapaikka
- Lempiurheilujoukkuetta

Skenaario

Pohdi kuvattua skenaariota ja käy loput kohdat läpi, kun olet valmis.

Olet kirjautunut läppäriisi valmistautuaksesi tärkeään projektiin. Järjestelmä pyytää sinua kirjautumaan sähköpostitiliisi uudelleen. Syötät käyttäjätunnuksesi, mutta saat "Väärä salasana" -virheilmoituksen. Kollegasi mainitsee kulkiessaan ohitsesi, että hän joutui vastaamaan erittäin kiireelliseen sähköpostiin eilen illalla.

Mitä sinä tekisit tässä tilanteessa?

- Oletko koskaan kokenut tilin lukkiutumista aiemmin?

- Mitkä olisivat välittömät toimenpiteesi?
- Kuka olisi yhteyshenkilösi? Keneltä voisit pyytää apua?

Keskustelu

Pohdi mitä olisi voinut tapahtua. Miksi järjestelmä vaati uudelleen kirjautumista? Miksi se ei onnistu?

Kertoisitko asiakkaillesi / organisaatiollesi, että sähköpostisi saattaa olla vaarantunut?

- Kyllä
- Ei

Neuvoja

Työ- ja henkilökohtaisten tilien suojaamiseen on useita hyviä käytäntöjä.

Vahvat salasanat: Käytä aina vahvoja salasanoja, jotka sisältävät yhdistelmän isoja ja pieniä kirjaimia, numeroita ja erikoismerkkejä. Vältä helposti arvattavia salasanoja, kuten syntymäpäiviä tai nimikirjaimia.

Uniikit salasanat: Älä käytä samaa salasanaa useissa eri tileissä. Jokaisella tilillä tulisi olla oma uniikki salasanansa. Tämä estää hakkerointia yhdellä murtautumisella.

Kaksivaiheinen tunnistautuminen: Ota käyttöön kaksivaiheinen tunnistautuminen kaikissa tileissä, joissa se on saatavilla. Tämä lisäkerros turvaa tiliäsi, vaikka salasana olisi hakkerin tiedossa.

Säännöllinen salasanan vaihto: Vaihda salasanasi säännöllisesti, esimerkiksi kerran puolessa vuodessa. Tämä vähentää riskiä, että salasanasi on vuotanut ja joutunut hakkeroinnin kohteeksi.

Tietoturvasovellukset: Käytä luotettavia tietoturvasovelluksia ja ohjelmistoja, kuten virustorjuntaohjelmistoja ja palomuureja, suojaamaan tietokonettasi ja mobiililaitteitasi haittaohjelmilta.

Varo huijauksia: Suhtaudu varauksella sähköposteihin, viesteihin ja verkkosivustoihin, jotka pyytävät henkilökohtaisia tietojasi tai salasanojasi. Varmista aina, että olet vuorovaikutuksessa luotettavan ja turvallisen lähteen kanssa.

Tiedon varmuuskopiointi: Varmuuskopioi säännöllisesti tärkeät tiedostot ja tiedot pilvipalveluihin tai ulkoisille kiintolevyille. Näin voit palauttaa tietosi, jos joudut tietovuodon tai tietojen menetyksen uhriksi.

Tietoisuus: Pysy ajan tasalla tietoturva- ja tietosuoja-asioista. Opettele tunnistamaan yleisiä tietoturvauhkia ja suojaustoimenpiteitä, jotta voit suojata itseäsi ja tietojasi paremmin verkossa.

Älä koskaan anna salasanaasi kenellekään.

Arviointi

Arvioikaa luottamustanne seuraaviin väittämiin asteikolla 1 - 5 (1 = 1 Ei lainkaan luottavainen, 5 = 5 Täysin luottavainen)

- Yrityksemme helpottaa käyttäjien salasanojen turvallista säilyttämistä esim. salasananhallintaohjelman avulla.
- Järjestämme säännöllisesti koulutusta, jossa korostetaan salasanoja koskevia parhaita käytäntöjä, esim. miten valita salasanat, joita on vaikea murtaa. Yksinyrittäjä: pidän itseni ajan tasalla osallistumalla webinaareihin ja koulutuksiin.
- Tietäisimme, jos salasanamme olisivat vaarantuneet.
- Tiedän keneen voin ottaa yhteyttä, jos sähköpostitilimme ovat vaarantuneet.

Johtopäätökset

On tärkeää ymmärtää salasanojen ja tilien suojaamisen merkitys sekä työ- että henkilökohtaisessa käytössä. Vahvojen ja uniikkien salasanojen käyttö, kaksivaiheinen tunnistautuminen ja tietoturvasovellusten hyödyntäminen ovat keskeisiä käytäntöjä, jotka auttavat suojaamaan tilisi tietomurroilta ja tietovuodoilta. Lisäksi tietoisuus huijausyrityksistä ja säännöllinen tietojen varmuuskopiointi ovat tärkeitä osia kokonaisvaltaista tietoturvaa. Pysymällä tietoisena tietoturvauhkista ja toteuttamalla asianmukaiset suojatoimenpiteet voimme pitää tietomme ja tilimme turvassa verkossa.