Uusi tutkimus paljastaa visuaalisen hakkeroinnin laiminlyönnin suojauksessa

Hakkeri tarvitsee usein tietomurtoa varten vain vähän suojattuja tietoja. Otsikoihin nousevat yleensä juuri suuret tietomurrot, mutta nykypäivän johtavat tietoturva-ammattilaiset ymmärtävät, että teknisesti yksinkertaiset uhkat voivat altistaa yritys- ja asiakastiedot laajoille vuodoille. Uudessa tutkimuksessa perehdytään arkaluontoisten, luottamuksellisten ja yksityisten tietojen urkintaan visuaalisella hakkeroinnilla. Visuaalinen hakkerointi on yhä merkittävämpi uhka, jota ei voi enää sivuuttaa.

Ponemon Institute toteutti Visual Privacy Advisory Councilin ja 3M Companyn, johtavan tietoturvasuojien valmistajan, toimeksiannosta 3M Visual Hacking Experimentin. Tutkimuksessa havaittiin, että lähes yhdeksässä kymmenestä tapauksesta (88 %) eettinen hakkeri (ns. white hat -hakkeri) sai urkittua työntekijöiden kirjautumistietoja ja muita yritystietoja visuaalisen hakkeroinnin keinoin esimerkiksi katsomalla pöydille jätettyjä asiakirjoja tai näytöillä näkyviä tietoja. Tutkimus osoitti, kuinka helposti arkaluontoisia tietoja voidaan urkkia vain visuaalisella hakkeroinnilla ja hyödyntämällä sekä työntekijöiden huolimattomuutta että yritysten puutteellista varautumista teknisesti yksinkertaisiin tietoturvauhkiin.

Muita 3M Visual Hacking Experimentin perusteella tehtyjä havaintoja:

Suojaamattomat laitteet ovat kaikkein alttiimpia arkaluontoisten tietojen visuaaliselle hakkeroinnille. Kokeen aikana eettinen hakkeri (luvallisesti toimiva henkilö, joka on palkattu paljastamaan tietoturvan heikot kohdat) esiintyi kahdeksassa yhdysvaltalaisessa yrityksessä alihankkijana tai osa-aikaisena työntekijänä yrittäen urkkia yritystietoja ollessaan muiden työntekijöiden näköpiirissä. Kokeen eri vaiheissa hakkeri huomasi, että tietokoneiden suojaamattomat näytöt ovat merkittävä riskitekijä. Yritykset olivat antaneet ennalta luvan kokeen suorittamiseen. **Hakkerin haltuunsa saamista arkaluontoisista tiedoista,** joita olivat esimerkiksi kirjautumistiedot, luottamukselliset tai salassapidettävät asiakirjat, talous- ja kirjanpitotiedot sekä vaitiolovelvollisuuden piiriin kuuluvat juridiset asiakirjat, **53 % oli peräisin suojaamattomilta laitteilta.** Hakkeri sai urkittua suojaamattomilta laitteilta enemmän tietoja kuin pöydiltä (29 %), tulostimista (9 %), kopiokoneista (6 %) ja fakseista (3 %) yhteensä. Työntekijöille on tärkeää järjestää koulutusta saatavilla olevista suojaustoimista, kuten urkinnan estämisestä tietoturvasuojien ja näytönsäästäjien avulla sekä valvomatta jätettävien laitteiden suojaamisesta salasanalla.

Visuaalinen hakkerointi

Teknisesti yksinkertainen hyökkäys, jossa valtuuttamaton taho pyrkii urkkimaan arkaluontoisia, luottamuksellisia ja yksityisiä tietoja.

Visuaalinen tietosuoja

Arkaluontoisten, luottamuksellisten ja yksityisten tietojen suojaaminen visuaaliselta hakkeroinnilta.

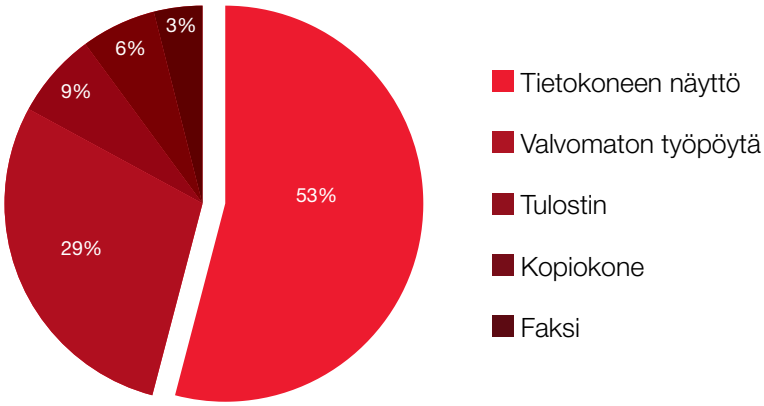
Hakkeroidut arkaluontoiset tiedot[1]:

- Kirjautumistunnukset ja -tiedot (47 %)
- Luottamukselliset ja salassapidettävät asiakirjat (35 %)
- Talous-, kirjanpito- ja budjettitiedot (12 %)
- Vaitiolovelvollisuuden piiriin kuuluvat juridiset asiakirjat (6 %)

Arkaluontoisia tietoja saatiin urkittua **88 %**:ssa tutkimuksen koetilanteista.[2]

Tietosuoja on paras käytäntö. | 3M

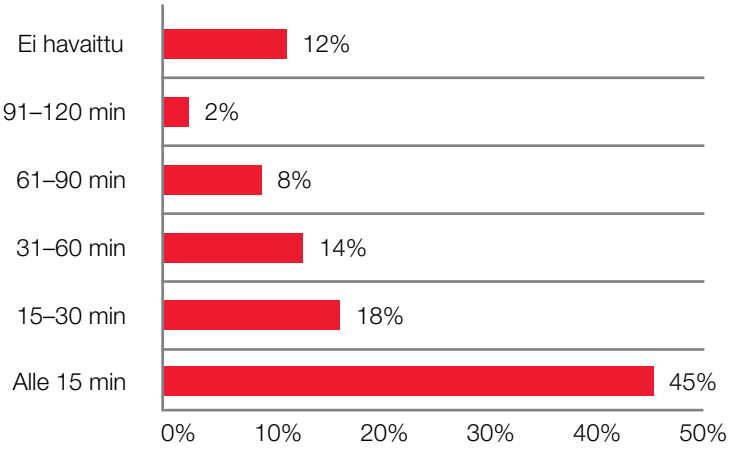
Arkaluontoisten tietojen hakkerointipaikat



Visuaalinen hakkerointi tapahtuu nopeasti ja usein täysin huomaamatta. Yritystietojen visuaaliseen hakkerointiin tarvitaan vain minuutteja. **Lähes puolet** (45 %) hyökkäyksistä kestää **alle 15 minuuttia** ja 63 % alle puoli tuntia. Riskiä kasvattaa entisestään se, että visuaalinen hakkerointi tapahtuu usein muiden huomaamatta. Kokeessa eettinen hakkeri yritti saada visuaalisen hakkeroinnin keinoin urkittua arkaluontoisia tai luottamuksellisia tietoja: hän kulki toimistotiloissa etsien näkyvillä olevia tai helposti saatavia yritystietoja, otti mukaansa luottamuksellisiksi merkittyjä asiakirjoja ja otti älypuhelimellaan kuvan tietokoneen näytöllä näkyvistä tiedoista. **Muut työntekijät eivät 70 prosentissa tapauksista puuttuneet asiaan edes silloin, kun hakkeri valokuvasi näytöllä näkyviä tietoja puhelimellaan.** Lisäksi hakkeri sai urkittua keskimäärin 2,8 tietokohdetta myös tilanteissa, joissa asiaan puututtiin. Muissa tilanteissa hän sai haltuunsa keskimäärin 4,3 tietokohdetta.

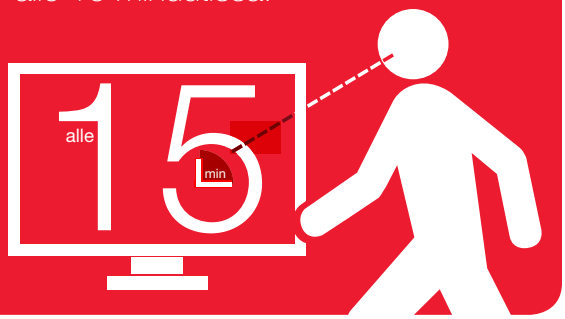
Ensimmäisen visuaalisen hakkeroinnin onnistumiseen tarvittu aika

n = 43 koetilannetta

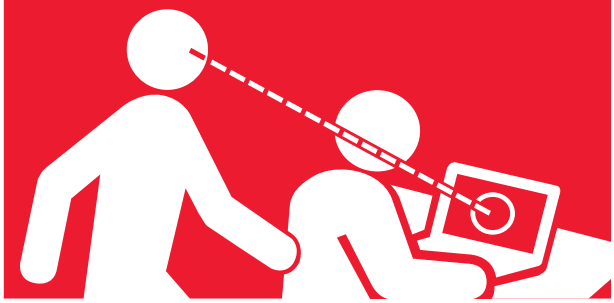


Visuaalinen hakkerointi onnistuu nopeasti.

Lähes puolet
hakkerointiyrityksistä
onnistui
alle 15 minuutissa.



70 %
hakkerointiyrityksistä
onnistui
muiden
puuttumatta
asiaan[4].



Tietosuoja
on paras käytäntö.

3M

Avokonttorit uhkaavat organisaatioiden visuaalista tietosuojaa.

Monissa organisaatioissa käytetään vapaampia ja avoimia työtiloja, joiden tarkoituksena on parantaa tuottavuutta. Yhdysvalloissa 70 % työntekijöistä työskentelee avokonttoreissa, jolloin toimittajien, ulkopuolisten tahojen ja jopa pahantahtoisten kollegoiden on hyvin helppoa nähdä luottamuksellisia tietoja laitteiden näytöiltä tai asiakirjoista.[5] Avokonttoreissa toteutetuissa kokeissa visuaalisen hakkeroinnin keinoin saatiin urkittua **keskimäärin 4,4 tietotyyppiä,** kun taas perinteisessä toimistossa luku oli 3,0. Avokonttoreiden yleistyessä entisestään yritysten on tärkeä varmistaa tietoturva laatimalla asianmukaiset tietosuojakäytännöt ja opettamalla henkilöstöä huomioimaan visuaalinen tietosuoja työhuoneen tai sermien ulkopuolella.

Visuaalisessa hakkeroinnissa sekä tietovuodoilla että niiden vaikutuksilla on merkitystä.

Usein työntekijät ja alihankkijat eivät tiedä käsittelemiensä tietojen kiinnostavan hakkereita. He eivät aina suojaa tietoja asianmukaisilla tavoilla tai estä niiden näkymistä ulkopuolisille. Kokeen aikana **visuaalinen hakkeri sai urkittua yhdessä koetilanteessa keskimäärin viisi tietokohdetta,** kuten työntekijöiden yhteystietolistoja (63 %), asiakastietoja (42 %), yrityksen taloustietoja (37 %), työntekijöiden kirjautumistunnuksia ja -tietoja (37 %) sekä henkilöstötietoja (37 %). Vaikka monet ymmärtävät luottokorttinumeroiden tai henkilötunnusten suojaamisen merkityksen, he eivät tiedä, että myös harmittomilta vaikuttavat tiedot, kuten yrityksen yhteystietohakemisto tai liiketoimintaan liittyvä kirjeenvaihto, voivat kiinnostaa hakkereita. Tällaiset tiedot voivat altistaa yrityksen laajamittaisille tietomurroille, joihin liittyy tietojenkalasteluhyökkäyksiä, talousvakoilua, sosiaalista hakkerointia ja jopa verkkokiristystä. Tietomurtojen estämiseksi on tärkeää korostaa työntekijöille kaikenlaisten tietojen suojaamisen merkitystä tallennuksen, siirron, käytön ja näyttämisen aikana.

Keskimäärin
5 yksityistä
tietokohdetta
paljastui[6].

Tietosuoja
on paras käytäntö.

3M

Yhteenveto

3M Visual Hacking Experiment paljastaa, kuinka helposti yritys voi joutua hakkeroinnin kohteeksi täysin huomaamattaan. Visuaalisen tietosuojan parantamiseksi on kuitenkin toimivia ratkaisuja. Yrityksissä, joissa käytettiin esimerkiksi 3M:n valmistamia tietoturvasuojia, visuaalinen hakkeri sai 50 %:ssa koetilanteista haltuunsa kolme tietotyyppiä tai vähemmän. Yrityksistä, joissa ei käytetty tietoturvasuojia, 43 %:ssa tapauksista visuaalinen hakkeri sai haltuunsa vähintään neljä tietotyyppiä.

Visuaalisen tietosuojan käytäntöjen laatiminen on tärkeä vaihe tiedotettaessa uhkista henkilöstölle ja alihankkijoille. Tietoturvasuojilla voidaan suojella arkaluontoisia tietoja käytön aikana, mutta tämän lisäksi yritysten tulee kouluttaa työntekijänsä käsittelemään tietoja vastuullisesti ja oikein. Tietoturvaa ja visuaalista tietosuojaa voidaan parantaa myös esimerkiksi noudattamalla puhtaan pöydän periaatetta, luomalla asiakirjojen tuhoamiselle oma prosessi sekä järjestämällä työntekijöille mahdollisuus ilmoittaa tilanteista, joissa he epäilevät visuaalista hakkerointia. Lisäksi on suositeltavaa suorittaa säännöllisesti koko organisaation kattava visuaalisen tietosuojan auditointi mahdollisten puutteiden tunnistamiseksi ja korjaamiseksi.

Käytäntöjen noudattaminen ei saa rajoittua toimistoon. Moniin tehtäviin liittyy etätyötä, ja henkilöt, jotka työskentelevät paljon toimiston ulkopuolella, ovat alttiina visuaaliselle hakkeroinnille, elleivät he pyri aktiivisesti suojaamaan tietoja. Liikkuvien työntekijöiden on tärkeää käyttää tietoturvasuojia. Tämän lisäksi yritysten täytyy määritellä selvästi, minkä tyyppistä tietoa on sallittua käyttää toimiston ulkopuolella, sekä luoda sopivat käytännöt tuottavuuden parantamiseksi yritystietojen suojauksesta tinkimättä.

3Mscreens.com/visualhacking

[1]Ponemon Institute, ”3M Visual Hacking Experiment,” 2015, rahoittajat 3M ja Visual Privacy Advisory Council.
[2]Ibid.
[3]Ibid.
[4]Ibid.
[5]International Management Facility Association.
[6]Ponemon Institute, ”3M Visual Hacking Experiment,” 2015, rahoittajat 3M ja Visual Privacy Advisory Council.

Tietosuoja
on paras käytäntö.

3M