IT SÄKERHETENS 10 BUDORD
TIETOTURVAN 10 KÄSKYÄ

1. HÅLL ERA PROGRAM UPPDATERADE
1. PIDÄ OHJELMISTOSI PÄIVITETTYNÄ

Största delen av uppdateringarna i dagens läge är till för att täppa hål i säkerheten.

Se till att era maskiner automatiskt uppdaterar operativsystemet och håll era andra program uppdaterade.

Suurin osa päivityksistä nykyään on tarkoitettu paikkaamaan turvallisuusaukkoja.

Varmista, että koneesi päivittävät käyttöjärjestelmän automaattisesti ja pidä muut ohjelmat päivitettyinä.

2. ANVÄND SÄKERHETSPROGRAM
2. KÄYTÄ TURVALLISUUSOHJELMIA

Skadeprogramsskydd eller 'Anti-Virus' har visat sig vara en av de effektivaste lösningarna för att bekämpa skadeprogram.

Använd ett program från en pålitlig leverantör och se till att bara ha ett säkerhetsprogram installerat på maskinen i gången, så att de inte krockar med varandra.

Haittaohjelmien suojaus tai 'Anti-Virus ohjelmat' on osoittautunut yhdeksi tehokkaimmista ratkaisuista haittaohjelmien torjumiseksi.

Käytä ohjelmaa luotettavalta tarjoajalta ja varmista, että koneessa on vain yksi turvallisuusohjelma asennettuna kerrallaan, jotta ne eivät törmää toisiinsa.

3. ANVÄND DIG AV STARKA LÖSENORD
3.KÄYTÄ VAHVOJA SALASANOJA

Lösenorden behöver inte vara en komplex blandning av stora och små tecken, symboler och siffror.

Sikta på något användarvänligt med minst 8 tecken. Använd inte samma lösenord två gånger. Pröva använda en nyckelhanterare för att hålla reda på era lösenord.

Salasanojen ei tarvitse olla monimutkainen sekoitus isoja ja pieniä kirjaimia, symboleita ja numeroita.

Tavoittele jotain käyttäjäystävällistä vähintään 12 merkillä. Älä käytä samaa salasanaa kahdesti. Kokeile käyttää salasanahallintaa pitääksesi kirjaa salasanoistasi.

4. AKTIVERA TVÅ-STEGS VERIFIERING / MULTI-FAKTORAUTENTISERING (MFA)
4. OTA KÄYTTÖÖN KAKSIVAIHEINEN TODENNUS / MONIVAIHEINEN TODENNUS

Två-stegs eller multi-faktorautentisering är en tjänst som möjliggör ett extra lager av säkerhet till inloggningsprocessen.

Utan MFA loggar man vanligtvis in genom att fylla i ett användarnamn och ett lösenord.

Genom att använda MFA kräver inloggningen ännu ett eller flera ytterligare lager av autentisering i form av till exempel en personlig PIN kod, en SMS kod eller ett fingeravtryck.

Kaksivaiheinen tai monivaiheinen todennus on palvelu, joka mahdollistaa toisen turvakerroksen kirjautumisprosessiin.

Ilman MFA:ta kirjaudutaan yleensä antamalla käyttäjänimi ja salasana.

Käyttämällä MFA:ta kirjautuminen vaatii vielä yhden tai useamman lisäkerroksen autentikointiin, esimerkiksi henkilökohtaisen PIN-koodin, tekstiviestikoodin tai sormenjäljen.

5. KLICKA FÖRSIKTIGT
5. KLIKKA VAROVASTI

Nätfiske, eller phishing, är vanligare än någonsin förr. I ett fiskeriförsök uppger sig anfallaren att vara någon eller någonting annat än den egentligen är.

Detta för att försöka lura offret att ge från sig känsliga uppgifter, klicka på en osäker länk eller öppna en fil som innehåller skadlig kod.

Detta leder oftast till ett krypteringsanfall eller missbruk av offrets betalmedel. Ungefär 90% av krypteringsanfall räknas härstamma från phishing.

Kalastelu eli phishing on yleisempää kuin koskaan aiemmin. Kalasteluyrityksessä hyökkääjä esittää olevansa joku tai jokin muu kuin mitä hän todellisuudessa on.

Tämä tapahtuu huijausyrityksellä, jolla uhri kehotetaan antamaan arkaluontoisia tietoja, klikkaamaan epäilyttävää linkkiä tai avaamaan tiedoston, joka sisältää haitallista koodia.

Tämä johtaa useimmiten salaushyökkäykseen tai uhrin maksuvälineiden väärinkäyttöön. Noin 90% salaushyökkäyksistä arvioidaan alkavan onnistuneesta kalastelusta.

6. SÄKERHETSKOPIERA REGELBUNDET
6. VARMUUSKOPIOI SÄÄNNÖLLISESTI

Om katastrofen ändå är framme och någonting sker med utrustningen, varken fysiskt eller med systemet så är det få saker som är till större hjälp än en ordentlig säkerhetskopia.

Det gäller också att ha koll på hur molntjänster säkerhetskopieras, vid exempelvis ett krypteringsanfall kan programvaran också kryptera filer i molnlagringen.

Säkerhetskopiering skall helst genomföras enligt 3-2-1 principen. Man bör alltid ha 3 kopior på sin data, säkerhetskopiorna bör lagras på minst 2 olika medier (Hårddisk/Extern Hårddisk/Molntjänst) och åtminstone 1 säkerhetskopia bör lagras off-site.

Jos katastrofi sattuu ja jotain tapahtuu laitteelle, oli se sitten fyysinen tai järjestelmään liittyvä, harvat asiat ovat suuremmaksi avuksi kuin kunnollinen varmuuskopio.

On myös tärkeää tietää, miten pilvipalvelut varmuuskopioidaan; esimerkiksi salaushyökkäyksessä ohjelmisto saattaa salata myös tiedostot pilvitallennuksessa.

Varmuuskopioinnin tulisi mieluiten noudattaa 3-2-1-periaatetta. Sinun tulisi aina säilyttää 3 kopioita tietojasi, varmuuskopioiden tulisi olla tallennettuna vähintään 2 eri medioihin (kiintolevy/ulkoinen kiintolevy/pilvipalvelu) ja ainakin 1 varmuuskopio tulisi säilyttää off-site.

7. FJÄRRHANTERA ENHETER
7. ETÄHALLITSE LAITTEITA

I dagens läge kan man förhindra att viktiga data hamnar i fel händer även om själva apparaten skulle göra det.

Med moderna verktyg kan man både spåra och tömma IT-utrustning som kommit bort.

Man kan också välja att endast ge rättighet till företagsdata från privat utrustning då vissa kriterier uppfylls. Till exempel krav på MFA, eller att maskinen måste ha skadeprogramsskydd aktiverat för att få åtkomst till företagsdata.

Nykyään voit estää tärkeiden tietojen pääsyn vääriin käsiin, vaikka itse laite päätyisi vääriin käsiin.

Nykyaikaisilla työkaluilla voit sekä jäljittää että tyhjentää kadonneen IT-laitteiston.

Voit myös valita antamaan oikeudet vain yritystietoihin yksityiseltä laitteelta, kun tietyt kriteerit täyttyvät. Esimerkiksi MFA-vaatimus tai vaatimus haittaohjelmien suojausohjelman käytöstä yritystietoihin pääsemiseksi.

8. KRYPTERING OCH HANTERING AV KÄNSLIG INFORMATION
8. SALAUS JA HERKKIEN TIETOJEN KÄSITTELY

Då man hanterar känsliga data som innehåller till exempel personuppgifter eller annan affärskritisk information är det skäl att använda sig av kryptering.

Om man växlar sådan information över e-post bör man skydda den med kryptering så att endast den avsedda mottagaren kan ta del av uppgifterna.

Lagrar man filer med kunduppgifter eller annan känslig information bör själva dokumenten också krypteras så att de bara kan läsas av personer med rätt behörighet.

Kun käsitellään herkkiä tietoja, kuten henkilötietoja tai muita liiketoiminnan kannalta kriittisiä tietoja, on syytä käyttää salausta.

Jos lähetät tällaisia tietoja sähköpostitse, sinun pitäisi suojata ne salauksella, jotta vain tarkoitettu vastaanottaja voi nähdä tiedot.

Jos tallennat tiedostoja asiakastiedoilla tai muilla herkillä tiedoilla, itse asiakirjat tulisi myös salata, jotta niitä voivat lukea vain oikeutetut henkilöt.

9. LOKALA NÄTVERKET
9. PAIKALLINEN VERKKO

Förutom alla åtgärder som kan göras på mjukvarunivå är det skäl att ha koll på hur själva nätverket är strukturerat.

En robust brandmur är det alltid skäl att ha. Med hjälp av förbestämda regler granskar brandmuren all inkommande IP-trafik och blockerar det som saknar behörighet.

Man bör också byta inloggningsuppgifterna till att utrustning. I många fall så kan inloggningarna till utrustningen fortfarande vara admin/1234, som direkt ur paketet.

Kaikkien ohjelmistotasolla tehtävien toimenpiteiden lisäksi on tärkeää tietää, miten itse verkko on rakennettu.

Luotettava palomuuri on aina syytä olla. Ennalta määrätyillä säännöillä palomuuri tarkistaa kaiken saapuvan IP-liikenteen ja estää luvattoman liikenteen.

Sinun tulisi myös vaihtaa laitteiden kirjautumistiedot. Monissa tapauksissa laitteiden kirjautumistiedot voivat olla edelleen admin/1234, suoraan pakkauksesta.

10. FYSISK SÄKERHET
10. FYYSINEN TURVALLISUUS

Sist men inte minst så skall man ha koll på säkerheten på det fysiska planet.

Vem har tillgång till utrustningen?

Vem kommer och går i utrymmena?

Viimeisenä muttei vähäisimpänä, sinun tulisi pitää huolta fyysisestä turvallisuudesta.

Kuka pääsee käsiksi laitteisiinn?

Kuka liikkuu tiloissa?

STAY SAFE!

Andreas Koschinski

EKM Service Ab Oy

0500 486 091

ak@ekm.fi

www.ekm.fi