Tampereen ammattikorkeakoulu
Tampere University of Applied Sciences

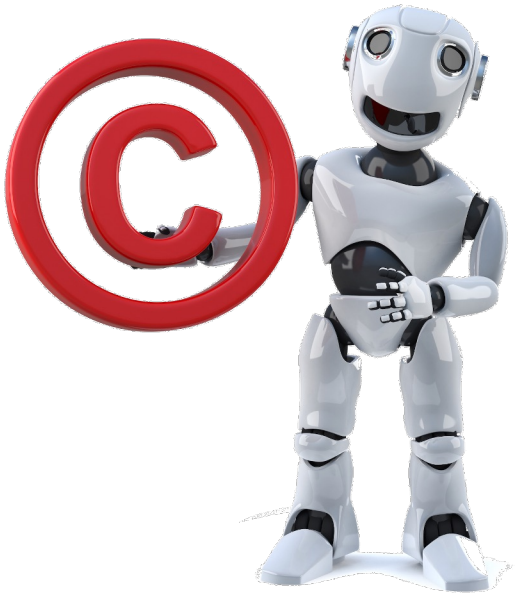
Automaation kyberturvallisuus

- 1- Tietoturva, perusteet

Kyy hanke
Mikko Korpela, Tampereen Ammattikorkeakoulu
Ville Haapakangas, Tampereen Ammattikorkeakoulu

Materiaalin oikeudet

- Materiaali on tehty osana OKM hanketta: *Kyberturvallisuuden opintokokonaisuudet* (Kyy)
- Copyright © *Tampereen Ammattikorkeakoulu; Mikko Korpela, Ville Haapakangas 2025*
- Käytetyt lisenssit :
  - Adobe Stock, Education License, Käytössä TUNI:n kautta
  - MS Powerpoint, Office 365, Käytössä TUNI:n kautta
- Käyttöehto:
  - Materiaalin käyttö sallittu vain opetuskäyttöön
  - Alkuperä mainittava



Kuva: AdobeStock,

Tampereen ammattikorkeakoulu
Tampere University of Applied Sciences

Tietoturva

- Tietoturva on osa kokonaisturvallisuutta, jonka keskiössä on tietoaineiston turvaaminen
  - Tietoriskienarviointi määrittää toimintamallit ja tekniset ratkaisut.
  - Oleellista, että tunnistaa mitä tietoa prosessissa syntyy tai käytetään ja mikä on sen merkittävyys
- Tietoturva on käsitteenä laaja ja se sisältää velvollisuuksia, vaatimuksia, toimintatapoja, määrityksiä ja teknisiä ratkaisuja.
  - Huomaa. Tekniset ratkaisut vain osa tietoturvan toteutusta!
- Tietoturva on osa johtamisjärjestelmää ja se pitää näkyä sen kaikilla tasoille
  - Arvot: Miten me haluamme toimia tietoturvan kanssa ja mikä tieto on arvokasta (missio, visio)
  - Strategia: Miten me saavutamme tietoturvan tavoitteet ja miten tietoturva näkyy toiminnassamme (Työkulttuuri)
  - Toteuttamiskeinot: Toiminnan suunnittelu, resursointi, dokumentointi, työkalut
  - Operatiivinen toiminta: Toiminnan kehitys, operatiiviset prosessit
- Hyvä tietoturva on kokonaisuus, jossa hyödynnetään teknisiä työkaluja
  - Se ei ole vahinko, eikä sitä voi suoraan ostaa

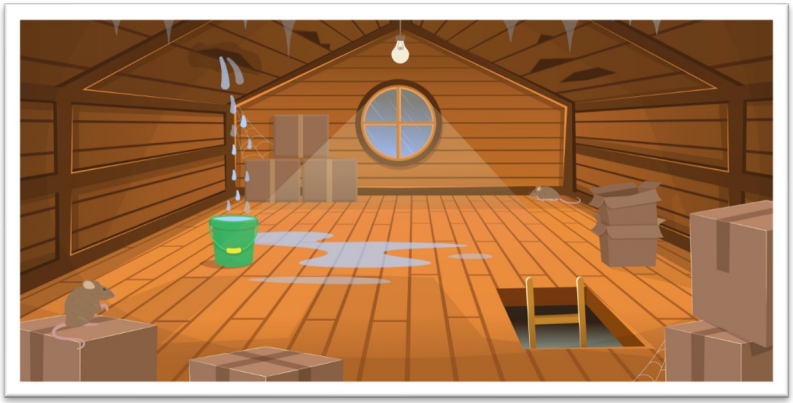
”Ei hätää me ulkoistimme tietoturvan”… Eli ulkoistitte osan johtoryhmän töistä?

Kuvat: AdobeStock, (Muokattu)

Tampereen ammattikorkeakoulu
Tampere University of Applied Sciences

Tietoturva

- Keskeisimpänä tavoitteena on luoda turvallinen tapa käsitellä tietoa.
  - Tietotekniikka ja tietoliikenne mahdollistavat tehokkaan tietojen käsittelyn. Eli se toteuttaa valittua politiikkaa ja käytänteitä
- Käytännössä tietoturva on hallinnollisia ja teknisiä ratkaisuja joilla varmistetaan
  - Tiedon LUOTTAMUKSELLISUUS: Tieto on oikeutettujen henkilöiden, toimijoiden ja järjestelmien käytettävissä, eikä sitä paljasteta tai saateta ulkopuolisten käyttöön
  - Tiedon EHEYS: Tietoa voi muokata vain oikeuden omaavat henkilöt, toimijat tai järjestelmät. Tieto ei muutu tai häviä virheiden, laiterikkojen tai luonnon ilmiöiden seurauksena
  - Tiedon SAATAVUUS: Tieto ja niiden muodostaman palvelut ovat oikeutettujen henkilöiden, toimijoiden ja järjestelmien käytettävissä riittävän nopeasti (Palveluvarmuus)
- Tietosuoja on juridinen termi, joka määrittää yksityisyyden suojaa ja henkilötietojen käsittelyä
  - Tietoturva on yksi keino toteuttaa tietosuojaa



Kuvat: AdobeStock,

Luottamuksellisuus

- Tieto on oikeutettujen henkilöiden, toimijoiden ja järjestelmien käytettävissä, eikä sitä paljasteta tai saateta ulkopuolisten käyttöön
- Käytännössä tämä tarkoittaa esimerkiksi:
  - Tunnistautumista: Kuka
    - Käyttäjätunnus + Salasana
    - Kaksivaiheinen tunnistautuminen (2fA)
    - Kulkukortti + PIN koodi
  - Rajoituksia / kontrolleja
    - Tiedon salaaminen (salakirjoitus)
    - Toimistohuoneen lukitseminen
  - Luottamusta / sopimuksia
    - Dokumentit palautetaan kassakaappiin
    - Tallennan tiedon sinne, minne sovitaan

Tekniikka

Tiedätkö minne omat tietosi voivat päätyä? – Kopiokone on tietoturvariski

Kopiokoneen kiintolevyt voivat tallentaa arkaluontoista tietoa. Kaikki yritykset ja yhteisöt eivät vielä ole havahtuneet tietoturvaongelmaan. Täyttä varmuutta ei ole esimerkiksi siitä, että Pohjois-Karjalan keskussairaalan monitoimilaitteiden tiedot hävitetään asianmukaisesti.

Lähde: YLE 24.7.2015

Kuvat: AdobeStock
Yle.fi

Tampereen ammattikorkeakoulu
Tampere University of Applied Sciences

Eheys

- Tietoa voi muokata vain oikeuden omaavat henkilöt, toimijat tai järjestelmät. Tieto ei muutu tai häviä virheiden, laiterikkojen tai luonnon ilmiöiden seurauksena
- Käytännössä tämä tarkoittaa:
  - Varmuuskopiointia (varautumista)
    - Kun jotain hajoaa!
    - Jos meitä kiristetään
    - Huomaa. Pilvipalvelu ei välttämättä ole varmuuskopio!
  - Käyttäjäryhmien määrittelyä
    - Katseluoikeus / muokkausoikeus
  - Sopimista / sopimuksia
    - Miten tieto kirjataan?
    - Esimerkiksi päivämäärä: Potilas kävi tarkastuksessa 05/10/2023
      - 5 päivä lokakuuta vuonna 2023?
      - 10 päivä toukokuuta 2023?

Esimerkki OVHcloud 2021

- OVHcloud on pilvipalveluja tarjoava yritys.
- Heidän tapa varmistaa tiedon eheys on tallettaa tallennettu tieto kahteen eri palvelinkeskukseen.
- Keväällä 2021 palvelinkeskus syttyi tuleen. Koska toinen palvelukeskus oli viereisessä rakennuksessa, tuhoitui samaan aikaan kaksi palvelinkeskusta.

Kyy –hanke

OVHcloud tulipalo 2021 (Ranska)
Lähde: Reurers 10.3.2021

Tays

Kuvantamisarkiston kuvia tuhoutunut tietojärjestelmäuudistuksessa Pirkanmaalla

29.1.2021 10:40:46 EET | Pirkanmaan sairaanhoitopiiri

Jaa

Pirkanmaan sairaanhoitopiirin ja kuntien käyttämän yhteisen kuva-arkiston tietojärjestelmäuudistuksessa on tuhoutunut potilaiden kuva-aineistoa. Kuvia on tuhoutunut pääasiassa niiltä henkilöiltä, joiden henkilötunnuksessa on ollut puute tai virhe. Potilaiden kuvista tehdyt lausunnot ja potilaskertomusmerkinnät ovat sen sijaan tallessa.

Lähde: Aamulehti 29.1.2021

Kuvat: AdobeStock
Aamulehti.fi

Eheys

Esimerkki OVHcloud 2021

- OVHcloud on pilvipalveluja tarjoava yritys.
- Heidän tapa varmistaa tiedon eheys on tallettaa tallennettu tieto kahteen eri palvelinkeskukseen.
- Keväällä 2021 yksi palvelinkeskus syttyi tuleen.
- Koska toinen palvelukeskus oli viereisessä rakennuksessa, syttyi myös toinen palvelinkeskus.
- Tulos:
  - Osa tiedosta menetettiin (vaikka niistä oli varmuuskopio)
  - Ranskan oikeus määräsi OVHcloud:n maksamaan korvauksia kahdelle asiakkaalle menetetystä tiedoista
- Mitä opittiin:
  - Tietoturva on kokonaisuus ja myös fyysinen ympäristö pitää huomioida
  - MUISTA! Digitaalinen data on aina fyysisesti jossain!

OVHcloud must pay damages for lost backup data

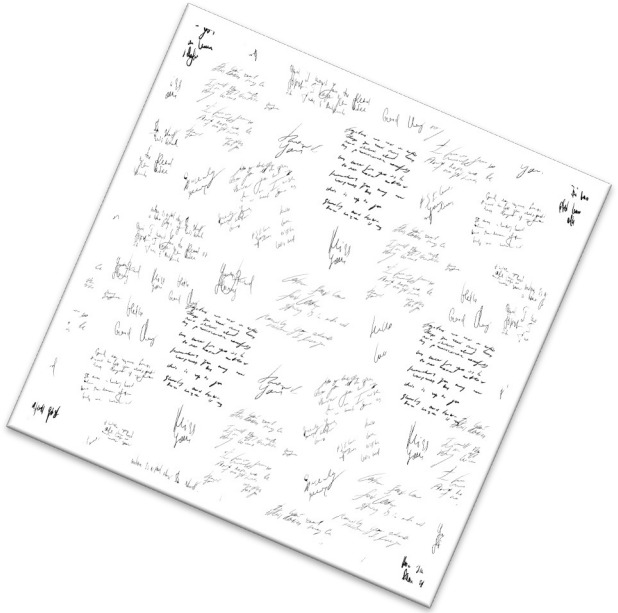
By **Chris Mellor** - March 23, 2023

A French court has ordered OVHcloud to pay damages to two customers who lost data in the 2021 fire at its Strasbourg datacenter.

Lähde: Blocks & Files
https://blocksandfiles.com/2023/03/23/ovh-cloud-must-pay-damages-for-lost-backup-data/

Saatavuus

- Tieto ja niiden muodostaman palvelut ovat oikeutettujen henkilöiden, toimijoiden ja järjestelmien käytettävissä riittävän nopeasti (Palveluvarmuus)
- Käytännössä tämä tarkoittaa:
  - Riittävän hyviä teknisiä ratkaisuja
    - Riittävän nopeita ja luotettavia tietoliikenneyhteyksiä
    - Tarkoitukseen soveltua ohjelmistoja
  - Varautumista… kun joku laite tai järjestelmä menee rikki
- Saatavuusongelma voi vaarantaa myös luottamuksellisuuden ja eheyden
  - Esimerkiksi suojattu ja salattu verkkolevy:
    - Verkkoyhteys on päivällä huono, joten
    - Päivällä saatu tieto kirjataan muistilehtiöön ja tallennetaan illalla
    - Luottamuksellisuus: Miten muistilehtiön paperit tuhotaan? Entä ruokatauko, kuka vahtii?
    - Eheys: Verkkolevyllä oleva tieto ei ole viimeisin. Mitenkäs epäselvä käsiala tai tulkinta?



Tekniikka on vain työkalu!

Kuvat: AdobeStock

Miksi se on hankalaa

- Tekniikka on monimutkaista (vahinkoja sattuu)
  - Outlook haavoittuvuus.
    - Lähettäjä pystyi määrittämään minkälaisen äänen sähköpostin saapuminen aiheutti.
    - Hyvä tarkoitus, mutta määrittely mahdollisti myös muunlaisen ohjelmakoodin syöttämisen
  - Rasberry Robin haavoittuvuus
    - Haittaohjelma kopioitui automaattisesti USB tikulle tai tikulta, kun se asennettiin tietokoneeseen
    - Levisi muun muassa valokuvaliikkeiden kautta
    - Perustui USB tikun käyttöä helpottavan ohjaimen hyväksikäyttöön.

HAAVOITTUVUUS 3/2023 CVSS 9.8 CVE-2023-23397

Kriittinen haavoittuvuus Microsoft Outlookissa

Päivitetty 16.03.2023 13:05 – Julkaistu 15.03.2023

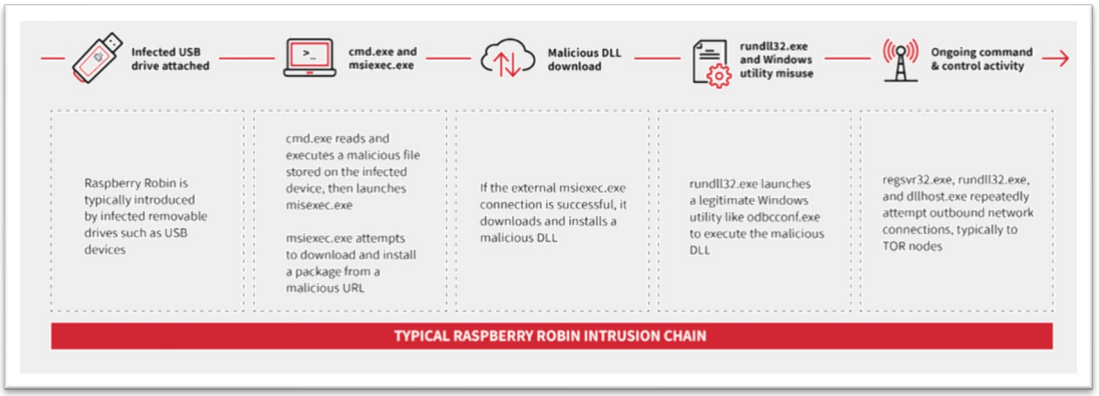
Microsoft tiedotti Outlookin vakavasta haavoittuvuudesta, jonka avulla on mahdollista korottaa käyttöoikeuksia. Haavoittuvuus mahdollistaa NTLM Relay -hyökkäyksen. Haavoittuvuutta hyödynnetään lähettämällä tietynlainen sähköpostiviesti Outlook-ohjelmaan. Hyökkäys aktivoituu sähköpostiviestin saapuessa Outlook-ohjelmaan jo ennen sähköpostiviestin avaamista tai sen esikatselua.

Lähde: Traficom CVSS 9.8
16.3.2023

Muista

- Päivitykset!
- Virustorjunta!
- Varmuuskopiot!

Lähde: Meltdown paper
https://meltdownattack.com



Lähde: red canary resources blog, 5.5.2022

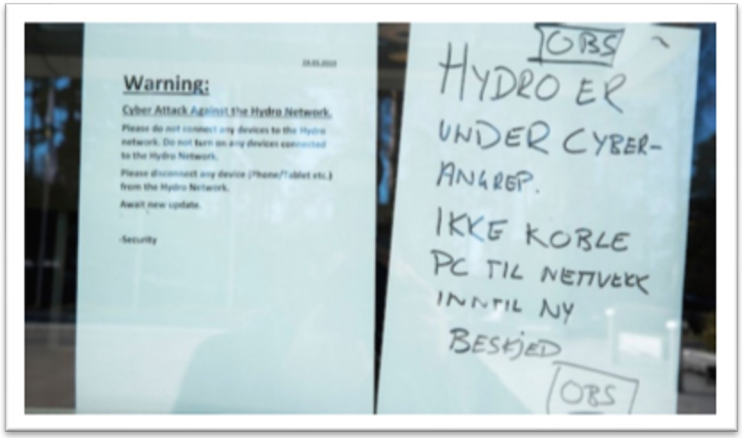
Miksi se on hankalaa

- Tasapainottelemme toiminnan ja uhkien kanssa
  - Esimerkki Taloushallinto
    - Taloushallinnon tehtävä on vastaanottaa laskuja
    - ”ÄLÄ AVAA .pdf tiedostoja”… Mutta miten sitten työ tehdään?
  - Esimerkki Norsk Hydro
    - Verkkohyökkäys pysäytti Norsk Hydron tuotannon maaliskuussa 2019
    - Kustannukset arviolta 71 milj €
    - Luotetulta asiakkaalta tuli sähköposti, jossa oli haittaohjelma, jonka avulla hyökkääjä pääsi yrityksen järjestelmiin

Mitä jos?

- Taloushallinto käyttäisi erillistä tietokonetta tulevan postin lukemiseen?
- Tietoturva on riskien hallintaa
  - Yhden laitteet käyttö kaikkeen, Joustava, mutta hankala hallita (suuri pinta-ala)
  - Monen laitteen käyttö, jäykempi, mutta helpompi hallita (pieni pinta-ala)

Lähde: ePressi, 9,6,2022

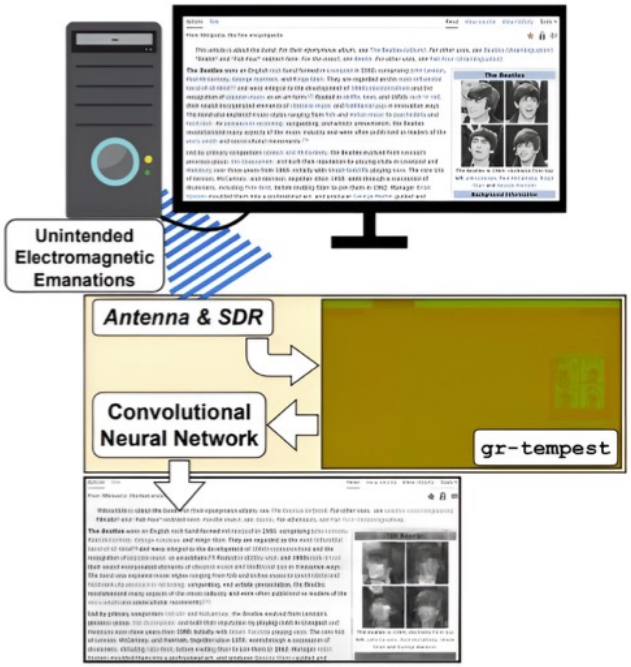


Lähde: Jari Seppälä, TAU

Miksi se on hankalaa

Sekamelskaan on helppo piilottaa

- HDMI kaapelin signaali voidaan lukea kaapeli ulkopuolelta
  - Miksi: Analoginen signaali aiheuttaa ympärilleen magneettikentän (Digitaalinen signaali on siirtotiessä analoginen)
  - Signaali on heikko, mutta AI työkalun avulla voidaan näytön kuva lähes palauttaa
- Pohdi? Kuinka helppo on sekaiselle pöydälle tai puhujapönttöön piilottaa ylimääräinen laite
  - Mitä ajattelet, kun kaapelin ympärillä on laite, jossa lukee ”Hälytin”



Tietoturva ei ole vain tekniikkaa ja bittejä.

- ”… ok. Avaan oven, että pääset tikkaiden kanssa korjaamaan lamput”

Lähde: Security researchers reveal it is possible to eavesdrop on HDMI cables to capture computer screen data, 30.7.2024
Kuva: Security researchers reveal it is possible to eavesdrop on HDMI cables to capture computer screen data, 30.7.2024
AdobeStock

Miksi se on hankalaa

- Koska ihmiset tekevät sen hankalaksi (hankalasti)
  - Esimerkki ”hyvästä” salasanasta
    - Älä käytä alle 10 merkin salasanoja
    - Salasanassa pitää olla isoja ja pieniä kirjaimia, numeroita ja erikoismerkkejä
    - Älä käytä nimiä, syntymäaikoja tai puhelinnumeroita
    - Älä käytä sanakirjan sanoja
    - Älä käytä sarjoja, kuten abcd tai 1234
    - Käytä aina eri salasanaa eri palveluissa
    - Älä kirjoita salasanaa mihinkään tai kerro kenellekään
  - Säännöt eivät voi olla mahdottomia
    - Kerrotaan mieluummin miten, kuin mikä on kiellettyä
  - Ihminen ei ole uhka vaan osa prosessia!
    - Hyvä tietoturva huomioi kaikki prosessin osat ja niiden heikkoudet (haavoittuvuudet)


DIGI & TEKNIIKKA | DIGIUUTISET

Kammottavia paljastuksia Vastaamon tietoturvasta

Myös Vastaamon salasanakäytännöt ovat olleet puutteellisia. KRP:n tietoteknisessä tutkinnassa selvisi, että potilasrekisterin käyttäjätunnuksella ”root” ei ollut lainkaan salasanaa.

Lähde: Iltalehti Digi & Tekniikka 27.9.2022


Harmittoman näköisten sovellusten synkkä salaisuus paljastui – ethän ladannut?

Tietoturva - 21.7.2022 21:49

Lähde: Iltalehti Digi & Tekniikka 21.7.2022


Zuckerberg's Social Media Accounts Hacked, Password Revealed as 'Dadada'

Facebook founder Mark Zuckerberg has had his Twitter, Instagram and Pinterest accounts briefly hacked at the weekend, according to various reports.

Lähde: NBC news 6.7.2017

Miten eteenpäin?

Tietoturva ei kuitenkaan (aina) ole vaikeata!

- Tekniset ratkaisut ovat vaikeita, mutta ne vain toteuttavat hallinnollisia päätöksiä

Tehdään asiat sovitusti, huolella ja tarkasti

- Tietoturva ei ole taikuutta, vaan työtä mitä tehdään ihan niin kuin muutakin työtä
- Muistetaan sen tavoitteet: Halu suojata ja hallita tieto-omaisuutta

Organisaation tulee varmistaa tietoturva, työntekijän pitää noudattaa sääntöjä!

- "Tein parhaan kykyni ja ymmärryksen mukaan" pitää riittää!
  - Koulutus ja harjoittelu!
- Virhe ei ole poikkeus vaan luonnollinen asia, joka pitää huomioida ennakkoon.
  - ”No se ei toimi, kun teit väärin” ei, kun ”Ahaa tuo pitääkin jatkossa huomioida, voitko auttaa siinä?”
- Hyvä organisaation toimii vastuullisesti ja kehittää toimintaansa jatkuvasti

Harjoittele, kehitä, verkostoidu, ole kiinnostunut!

Kuvat: AdobeStock,

Miten eteenpäin?

- Harjoittelu kannattaa, koska todellinen tilanne on vain ajankysymys
  - Muista, tekniikka pettää aina. Varmasti!
- Esimerkki: Tietoturvaharjoituksesta
  - Laita puhelin pöydälle ruutu alaspäin, et saa koskea siihen harjoituksen aikana
  - PAM! Kuvittele puhelin meni rikki
  - Miten toimin (Suunnittele)?
    - Onko tieto käytettävissä? (Saatavuus)
      - Yhteystiedot?
    - Pystytkö tunnistautumaan? (Luottamuksellisuus)
      - Pankki sovellus?
    - Onko tieto tallessa? (Eheys)
      - Kuvat?
  - Kehitä. Varmasti huomasit asioita, joita pitää kehittää

Ota harjoittelu mukaan toimintaan. 15 min kahvipöytäharjoitus on hyvä alku

- Mieti erilaisia skenaarioita ja mieti miten toimit niissä. Siis harjoittele ja varaudu, kun tosipaikka tulee!
- Esim: Valitkaa tuotannosta yksi laite, joka menee rikki
  - Miten rikkoutuminen vaikuttaa tuotantoon?
  - Miten uusi komponentti saadaan ja miten se asennetaan?
  - Mitä tietoa ja resursseja komponentin vaihto vaatii?

Kuvat: AdobeStock,