Cyber Security: 5 tips for bedre IT-sikkerhet

Digital sikkerhet er avgjørende for å beskytte virksomheter mot trusler og dataangrep. I denne guiden deler vi fem nyttige tips for økt data- og informasjonssikkerhet.

1 Sørg for god trådløs sikkerhet

Trådløse nettverk er helt avgjørende for at ansatte skal gjøre jobben sin. Men de trådløse signalene som sendes fra slike nettverk kan ha en lang rekkevidde, noe som gjør det vanskelig å vite hvem som faktisk prøver å koble seg på det.

Riktig kryptering av det trådløse nettverket er derfor kritisk. Her er våre råd til bedre trådløs sikkerhet:

- Aldri bruk standard passord på trådløse rutere eller andre enheter som kobles på nettet. De kriminelle vet hva standard passord er og søker etter enheter som ikke har byttet passordet.
- Skru alltid på kryptering, men pass på at krypteringstypen er WPA2 eller WPA3. Krypteringstypen WEP er svært usikker og bør ikke brukes.
- Endre standard nettverksnavn i den trådløse ruteren. Nettverksnavnet, for eksempel TelenorXXXXX, Getbox-XXXX eller Netgear-XXXX, kan noen ganger avsløre hvilken type enhet du bruker og gjøre det enklere å vite hvilke sårbarheter enheten har.
- Sett gjerne opp gjestenett og egne nettverk for smart-enheter og andre enheter du kanskje ikke stoler helt på. Dette gjør du i den trådløse ruteren. Husk at slike nettverk aldri bør gi tilgang til intern informasjon.
- Hvis det er mulig, sett opp automatisk oppdatering av den trådløse ruteren og alle enhetene som er tilkoblet. Hvis det ikke er mulig, lag en påminnelse om å gjøre dette manuelt. Kanskje du kan legge det inne som en kalenderpåminnelse den første dagen i hver måned?

2 Lag gode passord og aktiver totrinnsverifisering

Passordene dine kan fort komme i feil hender, for eksempel hvis uvedkommende får tak i dem gjennom phishingangrep, sosial manipulering eller angrep der de «gjetter» seg frem til ulike kombinasjoner av bokstaver og tall til de finner det riktige. Derfor er det kritisk at du lager gode passord som er vanskelige å knekke, lette å huske og at du aktiverer totrinnsverifisering på tjenester for å styrke sikkerheten om passordet skulle komme på avveie.

Passord

Gode passord er en forutsetning for å unngå at noen enkelt kan gjette seg frem til hva det er. Med disse enkle grepene, kan passordene fort bli mye vanskeligere å knekke:

- Passordet bør være en frase eller setning, for eksempel fra en bok eller en sang. Fraser og setninger er enklere å huske enn tilfeldige tall og bokstaver.
- Passordet bør være langt. Jo lengre det er, jo vanskeligere er det å gjette seg frem til. En frase bør være minst fem ord eller 16 tegn.
- Ikke bruk det samme passordet over alt. Vi har mange passord, og det er vanskelig å lage og huske unike passord for alle tjenester. Du bør likevel velge unike passord der det er ekstra viktig, for eksempel på epost, i jobbsystemer og der du har lagret betalingsinformasjon.
- Bytt passordet hvis du får varsel eller oppdager mistenkelig aktivitet på noen av dine konti. Noen ganger kommer passordene på avveie som en følge av et datainnbrudd. Når du får varsel om det, må du bytte passordet i alle tjenester du har brukt akkurat dette passordet så snart som mulig.
- Bruk gjerne en passordhåndterer (password manager) slik at du kan få oversikt over alle dine konti samt unike og gode passord på alle tjenester.

Totrinnsverifisering

Noen ganger kommer dessverre passordene våre på avveie, og da vil totrinnsverifisering styrke sikkerheten betydelig.

Totrinnsverifisering er en kombinasjon av:

- noe du vet (for eksempel brukernavn og passord) og / eller
- noe du har (for eksempel telefon eller nøkkelbrikke) og / eller
- noe du er (for eksempel fingeravtrykk eller ansiktsgjenkjenning)

Totrinnsverifisering innebærer at du, i tillegg til å skrive inn et passord, mottar en engangskode via SMS, en app, en sekundær epost, verifiserer kode med nøkkelbrikke eller bruker biometri for å verifisere at du er den du er, når du logger på en konto. Passordet bør være en frase eller setning, for eksempel fra en bok eller en sang. Fraser og setninger er enklere å huske enn tilfeldige tall og bokstaver.

Du bruker sannsynligvis allerede totrinnsverifisering, for eksempel i nettbanken din (Bank-ID), men har du tatt dette i bruk på tjenester som LinkedIn, Facebook, Twitter eller din epostkonto? Husk at epostkontoen er den aller viktigste kontoen å sikre med to-faktor. Grunnen til dette er at dersom du glemmer passordet til kontoen din, så blir forespørselen om å resette passord vanligvis sendt til epostkontoen din.

Passord på avveie?

Lurer du på om passordet ditt har kommet på avveie? Gå inn på nettsiden haveibeenpwned.com og skriv inn din epostadresse. Dersom e-post adressen din har blitt kompromittert i et angrep eller lekkasje, ser du informasjonen der. Det er viktig at passordet er endret på eventuelle tjenester der dette har blitt avdekket.

3 Lås enhetene dine

En ulåst PC, mobiltelefon, nettbrett eller andre enheter kan bety at uvedkommende kan få tilgang til verdifull informasjon, uten at de legger igjen noen spor.

Vi anbefaler:

- Bruk alltid passord, pinkode eller biometrisk kode på enhetene dine.
- Lås alltid enheten når du går fra den, selv om det bare er en kort tur på toalettet.
- Sett på automatisk låsing etter noen få minutters inaktivitet.
- Sørg for at ikke andre får tak i koder eller passord til enhetene.
- Ser du en enhet som er åpen, lås den og gi eieren en liten påminnelse.

4 Opptre sikkert på sosiale medier

Det ligger i vår natur at vi ønsker å dele, men er det alltid lurt? Ved bruk av sosiale medier bør du tenke over følgende:

- **Informasjon kan bli misbrukt:** Det er lite vi selv kan gjøre for å forhindre at informasjon vi legger ut kan bli misbrukt. Vi må derfor vurdere om det som legges ut kan bli misforstått eller brukt til andre ting enn det som var tiltenkt.
- **Informasjon blir aldri borte:** Det som publiseres på nett blir aldri helt borte. I noen tilfeller kan tjenester som Slettmeg.no hjelpe til med å få ting fjernet, men husk alltid på at et delt innlegg kan være nærmest umulig å fjerne helt.
- **Startstedet for hackere og angripere:** De som ønsker å bryte seg inn i IT-systemer, bruker ofte informasjon som er tilgjengelig på sosiale medier. Kanskje du får en troverdig epost fra en du kjenner godt, men som faktiske kommer fra noen som har funnet informasjon om deg og vennene dine på sosiale medier.
- **Identitetstyveri:** Informasjon om deg på sosiale medier kan være nok til at en annen kan overta din identitet. Der finnes historikk, relasjoner, bilder og annen informasjon som gjør det enklere for en annen å utgi seg for å være deg.

5 Ivareta sikkerheten på hjemmekontoret

Mange av oss arbeider fortsatt hjemmefra, og det kan se ut til at det vil fortsette å være slik en stund til. Når du sitter på hjemmekontor, befinner du deg delvis utenfor den digitale og fysiske sikkerheten du vanligvis har på kontoret. Derfor er det viktig å ta noen forholdsregler, slik at du sikrer arbeidet så langt det lar seg gjøre.

Et av de viktigste tiltakene du kan gjøre, er å undersøke om uvedkommende har fått tilgang til det trådløse nettverket ditt. Konsekvensene av en slik uønsket tilgang kan nemlig både være tregere nettverkshastighet og at noen får tilgang til dataene dine, uten at du ønsker eller vet om det.

For å få oversikt over dette finnes det flere gode løsninger som kan benyttes, blant annet en modul som heter Fingbox, som kan se hvilke enheter som er på nettverket og varsle dersom ukjente enheter dukker opp. Det er også mulig at din router har god funksjonalitet for dette, som du kan undersøke med trinnene under, men denne framgangsmåten kan nok framstå litt vel teknisk for noen:

1. Logg inn i administrasjonspanelet på den trådløse ruteren din. Dette gjør du ved å taste inn ruterens IP-adresse i adressefeltet i nettleseren på en maskin tilkoblet det aktuelle nettet. Dersom du ikke kjenner IP-adressen, kan du søke opp «CMD» i Windows-søkefeltet og åpne applikasjonen. Det vil da dukke opp et svart vindu («command prompt»). I dette vinduet skriver du inn «ipconfig/all», i ett ord, uten «». Trykk Enter. Det vil nå dukke opp en del informasjon. Let etter linjen som heter «Default Gateway». Bak navnet står den aktuelle IP-adressen. På Mac: Åpne Terminal. Du finner Terminal enten ved å søke opp programmet i søkefeltet eller ved å lete blant apper. Tast inn «route get default», uten «». Trykk Enter. Let etter linjen «gateway». Der finner du ruterens IP-adresse.
2. Skriv inn IP-adressen i adressefeltet i nettleseren din, inkludert alle punktum. Trykk Enter.

3. Dersom IP-adressen var korrekt, skal du nå få beskjed om å logge inn med brukernavn og passord. Du finner ofte brukernavn og passord til administrasjonspanelet skrevet på baksiden av ruteren din. Logg inn med brukernavn og passord (enten standardpassordet du finner på ruteren eller det nye passordet du eller noen i husstanden har laget selv). Dersom ruteren fortsatt er konfigurert med standardpassord, bør du endre det også.

4. Når du har logget deg inn i administrasjonspanelet, bør du lete etter et menyalternativ som omhandler tilkoblede enheter, for eksempel Device Manager, Connected Devices, My Network, eller lignende. Trykk på det aktuelle menyalternativet.

5. Her skal du få opp en oversikt over alle tilkoblede enheter på nettverket. Du finner både mobiltelefoner, PCer, nettverktstilkoblede TVer og andre enheter som bruker det trådløse nettverket i denne oversikten. Undersøk om noen av de tilkoblede enhetene ikke tilhører husstanden.

6. Dersom du mistenker at noen av enhetene ikke hører hjemme på nettverket, bør du dobbeltsjekke at du har skrudd på WPA2-kryptering på nettverket. Deretter må du endre passordet på både ruteren (det du brukte for å logge inn i administrasjonspanelet) og nettverkspassordet (det du bruker for å koble deg til det trådløse nettet). Husk å ta vare på passordene på en trygg måte, for eksempel i en passordhåndterer som nevnt tidligere, og husk å lage sterke passord! Når du endrer nettverkspassordet vil alle enheter som bruker det trådløse nettet bli kastet ut og du må deretter logge disse på igjen via nettverksinnstillingene på de aktuelle enhetene.

Experis Cyber Security – Din sikkerhetspartner

Hvis uhellet skulle være ute, ta kontakt med eksperter internt eller eksternt og vær ærlig om hva som har skjedd. Kun da kan du redusere omfanget av hendelsen så mye som mulig.

Trenger du hjelp til å gjøre sikkerhetsarbeidet i virksomheten bedre og mindre ressurskrevende? Experis er spesialister i slike digitale sikkerhetstjenester og tilbyr virksomheter hjelpen de trenger for å håndtere alle deler av sikkerhetsarbeidet.

- **Rådgivning:** Vi hjelper deg med sikkerhetsledelse.
- **Testing:** Vi finner sårbarheter før andre gjør det.
- **Overvåking:** Vi oppdager cyberangrepene før de gjør skade.
- **Arkutektur:** Vi designer for at du skal være godt sikret mot interne og eksterne trusler.
- **Opplæring:** Vi sørger for at dere har kompetansen dere trenger.

Ta gjerne kontakt med oss i dag, slik at du er bedre rustet til å håndtere morgendagens sikkerhetsutfordringer. Vi ser frem til å finne gode løsninger basert på dine ønsker og utfordringer.

Om Experis

Experis er et ledende norsk IT-konsulentselskap med mer enn 700 konsulenter og partnere. Selskapet har lang erfaring med prosjekt- og løsningsleveranser innen IT til både offentlig og privat sektor. Selskapets fag- og bransjekompetanse i kombinasjon med velprøvde metoder og prosesser skaper trygge, forutsigbare rammer både for smidige, nyskapende og mer tradisjonelle prosjekter.

Experis har erfarne konsulenter innen teknologiledelse, med bakgrunn som rådgivere, ledere og fagspesialister. Gjennom rådgivning, utvikling og forvaltning av digitale løsninger forenkler vi morgendagen. Les mer på experis.no.

En driver for digital transformasjon

Teknologi utvikler seg hele tiden. Det gjør også ferdigheter og kompetanse som følger med. Experis er en partner som støtter opp når kundene tilegner seg, tar i bruk og får resultater gjennom teknologi. Vi besitter fleksibel ekspertise og har bransjespesifikke forretningsløsninger.