Grant Thornton

An instinct for growth™

Guide til god cybersikkerhed

Hvis du har spørgsmål, er i tvivl om emner eller virksomhedens cybersikkerhed og modenhedsniveau, så kontakt:
Anders Grønning-Kjærgaard
Director, Head of IT Audit and Advisory
T +45 35 27 50 53 • E anders.kjaergaard@dk.gt.com

Adgangskoder til beskyttelse af dine data

Adgangskoder er en gratis, nem og effektiv måde at beskytte sig mod uautoriserede adgang til jeres systemer og informationer.

- Kryptér jeres computere med en adgangskode ved opstart. Brug også de biometriske muligheder på telefoner og tablets.
- Brug eventuelt to-faktor godkendelse når I benytter hjemmesider til fx webbank og webmail.
- Undgå forudsigelige adgangskoder. Brug gerne flere ord, der giver mening for netop dig, fx 17Ber!inTri, hvis Berlin triatlon i 2017 betød noget for dig.
- Hvis du bruger stærke adgangskoder som ovenfor, så minimer antallet af gange adgangskoder skal ændres. Skift kun hvis der er mistanke om at brud på sikkerheden.
- Skift leverandørens standard adgangskode ved indkøb af nye systemer.
- Giv medarbejdere mulighed for at benytte værktøjer til sikker opbevaring af adgangskoder.

Minimer skaden ved en ondsindet kode

En ondsindet kode kan ramme alle. Din virksomhed kan beskyttes med simple tiltag uden store omkostninger.

- Brug anti-virus programmer på jeres compturere. Installer kun godkendte app's på jeres mobile enheder og begræns medarbejdere i at kunne downloade og installere ukendt software.
- Opdater jeres software, styresystemer og firmware så hurtigt og ofte som muligt. Brug 'Automatisk opdatering' hvis det er muligt.
- Fjern muligheden for at bruge USB-stiks og hukommelseskort. Giv medarbejderne mulighed for at overføre data via (krypteret) mail og cloud-løsninger.
- Aktiver firewall – både den i jeres netværk og den (oftest gratis og indbyggede) i styresystemet så der skabes en sikker buffer mellem jeres enheder og Internettet.

Beskyt jeres mobile enheder

Mobile enheder, der bruges udenfor kontoret og hjemmet kræver mere beskyttelse end stationært udstyr.

- Aktiver PIN/adgangskode/biometrisk beskyttelse på enhederne.
- Aktiver sporing på enheden, så enheden kan blive fundet, slettet eller låst, hvis den mistes.
- Opdater jeres app's og system ofte. Slå eventuelt automatisk opdatering til.
- Undgå at bruge offentlige trådløse netværk. Brug enten 3G eller 4G via mobiludbyder eller VPN hvis muligt.
- Udskift gammelt udstyr hvis det ikke understøttes af leverandøren.

Tag backup af jeres data

Tag periodisk backup af jeres data og test at de kan genskabes indenfor rimelig tid. Dette vil reducere jeres 'nedetid' i forbindelse med tyveri, brand, anden fysisk skade eller ransomware.

- Identificer hvilke data, der er kritisk for jeres virksomhed og som I skal have en sikkerhedskopi af. Dette kan være mail, dokumenter, kundedatabase, økonomisystem, kontakter osv. Sørg for at backup er en daglig rutine – både udførelse og kontrol.
- Test periodisk at I kan genskabe data fra backup. Data, der ikke kan genskabes fra backup er tabt data.
- De medier, der indeholder backup, fx ekstern disk skal kun være tilsluttet virksomhedens netværk når der skal tages backup. Ellers skal den gemmes er sikkert sted. Overvej om en cloud-baseret backupløsning er mulig.

Undgå 'Phishing-angreb'

'Phishing-angreb' er angreb mod virksomheden med det formål at få adgang til penge. Typisk i form af mails, beskeder fra banken eller pop-ups. Kan både være 'Den nigerianske prins', men også RansomWare.

- Begræns medarbejderens rettigheder på computeren. Hvis medarbejderen ikke kan installere software kan angriberen heller ikke. Dette kan reducere omfanget af et succesfuldt angreb.
- Scan computere og servere for ondsindet kode, fx virus og malware. Skift adgangskoder hvis der er mistanke om et angreb. Straf ikke medarbejdere hvis der er sket et angreb. Ros dem for at opdage det og fortælle det.
- Lær dine medarbejdere at spotte 'Phishing-angreb'. Se efter dårlig grammatik, stavning eller links, der ikke peger derhen hvor de skal. Uddan nøglemedarbejdere i hvordan de spotter mere målrettede angreb, som fx en sms fra en chef, der beder om straksoverførelser.