Campus Bornholm

IT-sikkerhed

Håndbog for medarbejdere

Version: 10. december 2020

Indholdsfortegnelse

1 Indledning

1.1 Forord

Denne håndbog har til formål at oplyse medarbejdere om de IT-sikkerhedsprocedurer og -planer der anvendes på skolen. Medarbejderne skal have indsigt i procedurerne/planerne, da viden herom, er medvirkende til korrekt adfærd og håndtering.

1.2 Formål

Det overordnede formål er, at opretholde den fornødne sikkerhed omkring IT-systemerne og deres data, og undgå:

- Datatab og -læk
- Uvedkommendes adgang til data
- Hackerangreb

1.3 Ansvar og pligt

For at opretholde sikkerheden, skal håndbogens anbefalinger kendes og efterleves.

- CB har til pligt at træffe fornødne dispositioner, for opretholdelse af sikkerheden og gældende lov (GDPR).
- Alle medarbejdere har pligt til at melde om forhold der strider mod reglerne, eller mistænkelige forhold i øvrigt.

Ved større sikkerhedsbrud, aktiveres "Incident Response Plan" af ledelsen.

1.4 Øvrige instrukser og områder

Hvor det har IT-mæssig relevans, behandles også forhold under andre sikkerhedsområder.

Følgende instrukser ligger på INTRA: (https://intra.cabh.dk)

- Regnskabsinstruks
  Omhandler indskærpede procedurer og sikkerhed omkring økonomiske systemer. Medarbejdere, der håndterer økonomi, skal kende og efterleve denne.
- Persondataforordningen (GDPR)
  Omhandler alle forhold omkring persondata.
- Beredskabsplan
  Generelt forhold

IT beredskabsstrategi og -plan foreligger til ledelsesbrug.

IT-vedledninger og Information ligger på IT. (https://it.cabh.dk)

1.5 Datasikkerhedsorganisation

Internt sikkerhedspersonale udgøres af rollerne:

- Dataansvarlig: Direktør (Vicedirektør)
- Uddannelsesansvarlige: Uddannelseschefer
- HR-ansvarlig: Ressourcechef
- IT-ansvarlig: IT-koordinator
- Lokale Datakontaktperson: IT-koordinator

Eksternt tilknyttede sikkerhedspersoner:

- DPO[1]: EFIF-ansat konsulent

[1] En, over for Campus Bornholm, uafhængig person, hvis opgave det er, at rådgive og føre tilsyn med GDPR. Anvisninger og påbud fra denne, skal følges.

2 Definition af fjendebilledet

2.1 Uvedkommende

Enhver person der ikke er godkendt til indsigt i, eller behandling af, en given oplysning, sag eller område, defineres som ”uvedkommende”. Uvedkommende er også – ellers godkendt – personale, der ikke har brug for at vide noget om emnet.

2.2 Trusselsniveau

Forsvarets Efterretningstjenestes ”Center for Cybersikkerhed” advarer om, at trusselsniveauet aldrig har været højere end nu. Der er dagligt nyheder om (store) virksomheder, der er blevet hacket.

Næsten al data og kommunikation, samt styrings- og sikkerhedsudstyr, er IT-baseret. Adgang hertil er derfor mål for automatiseret hackerangreb. Hackerne har til formål at trænge ind, for at:

- Stjæle oplysninger og/eller
- Låse (kryptere) alle filer vha. ”ransomeware”.

Virksomheder verden over udsættes dagligt herfor (også vi), og målet er pengeafpresning eller spionage.

Hackerne betragter medarbejderne som det svageste led

Hackerne går målrettet efter at narre virksomhedens medarbejdere, for at få adgang. Det gør de med falske mails, websider m.m.

Vores bedste værn er velinformerede og veluddannede medarbejdere

2.3 Awarenes

For at give vores medarbejde de bedste arbejdsbetingelser i forhold til opretholdelse af den fornødne IT-sikkerhed, er det obligatorisk, at de gennemfører et online kursusforløb, der gør dem opmærksomme (aware) på de trusler der foreligger, og hvordan de håndteres.

3 Sikkerhedsprocedurer

3.1 Netværk

3.1.1 Fysisk netværk

Serverrum og skabe med krydsfelter og switche er aflåst. Kun nødvendige netværksudtag i lokalerne, er aktive.

3.1.2 Trådløst netværk

Der anvendes følgende trådløse netværk:

- CB For privatejede computere (certfikat-krypteret)
- CB domain For CB's computer (certfikat-krypteret)
- CB guest Gæstbrugere

Ansatte og elever har adgang til det trådløse netværk, i kraft af deres login. Kun så længe man er ansat eller studerende, har man adgang.

"CB guest" kræver særlig kode, der oplyses af IT. Koden må ikke oplyses til elever, da internetspærring under eksamen derved kan omgås (og nogle gange sker det uden elevens vidende). "CB guest" har svag kryptering, og har ikke fornøden adgang til ressourcer i netværket. Det må derfor ikke benyttes til almindelig brug.

3.1.3 Andre trådløse netværk

Undlad at bruge åbne netværk, hvor der ikke skal logges på. Brug i stedet for Internetdeling på din telefon.

3.1.4 Udskrivning

Udskrivning sker til centralt opstillede kopimaskine, fra hvilke et udskriftsjob kan trækkes vha. låsekortet. Vi kalder det "Folllow Me". Det sikrer, at fx følsomme ting ikke ligger og flyder i bakkerne.

3.2 Login-konto

Passwords består af 12 komplekse karakterer, og for Microsofts sky-tjenester (mail og Teams), sendes der regelmæssigt en SMS for ekstra autentifikation (multifaktor).

- Password gælder for et år ad gangen. Når de skal skiftes, får du besked. Du kan se i https://perssys.efif.dk hvornår det skal skiftes.
- Forlad aldrig en computer, hvor du er logget på. Lås den. Når du går hjem, skal den slukkes.
- Skift dit password hvis du har mistanke om, at andre har fået adgang til den.

Der har tidligere været tilfælde, hvor kriminelle har haft held med at stjæle en identitet, fordi password'et var for nemt, og blev gættet. Da man nu havde adgang til mailkontoen, kunne man nemt nulstille passwords for andre tjenester, fordi link om nulstilling blev sendt til ens mail-adresse.

3.3 Arbejdscomputer

3.3.1 Sikring

Computeren er sikret mest mulig, og den kan ikke anvendes uden logon. Efter strømbesparende tilstand (dvale) eller låsning, kræves password.

Harddisken er krypteret (bitlocker), og kan – selvom den bliver taget ud – ikke læses af uautoriserede.

Vi anvender Windows-computere, bla. fordi de har et ekstra netværksmæssigt sikkerhedslag, hvor sikkerheden kan styres fra centralt hold.

3.3.2 Sikkerhedsopsætning

Der må ikke ændres på computerens sikkerhedsopsætning. Antivirus må ikke frakobles og der må ikke installeres anden antivirus-software, driveropdaterings- eller systemoptimeringsprogrammer.

3.3.3 Sikkerhedsopdateringer

Computeren skal holdes sikkerhedsmæssigt opdateret. I de fleste tilfælde kommer der meddelelse om det, men ikke altid. Gå derfor ind i "SoftwareCenteret" og se status og foretage opdatering derfra.

3.3.4 Sluk din computer

Operativsystemet har brug for, at computeren slukkes/genstartes – ellers kan den ikke sikkerhedsopdatere.

3.3.5 Netværksadgang

Computeren logger automatisk på vores trådløse netværk.

Tager du computer med hjem eller på rejse, kobler computeren op til EFIF's netværk vha. "Direct Access". Det sker uden du mærker det. Men pas derfor godt på din computer, når du er på rejse.

3.3.6 Computeren er til arbejdsmæssige formål

Brug ikke computeren til formål, den ikke er beregnet til. Ved at installere ukendte programmer, spil, m.m. kan computerens funktionalitet blive beskadiget.

3.3.7 Lån aldrig din computer ud

Computeren er dit primære arbejdsredskab, og meget arbejde kan gå tabt. Lån den ikke ud – heller ikke til børn, familie m.fl.

3.3.8 Bortkomst

Hvis du mister din computer, skal du omgående (straks) melde det. Også selvom det er weekend eller ferie. Computeren er nøglen til Campus Bornholms netværk, og dem vi hostes hos. Computeren har – med de rigtige login-oplysninger – adgang til alle de systemer, som vi er tilknyttet, og computeren kan tilgå disse overalt i verden. Når IT-administrationen får besked, kan computerens adgang spærres.

3.4 Arbejdsmobiltelefon

3.4.1 Sikring

Telefonen er sikret mest mulig, og der anvendes sikkerheds-, og PIN-kode samt biometri. Der oprettes AppleID til arbejdsbrug for hver bruger, og funktionen "Find my iPhone" er aktiveret.

Disse ting må ikke slås fra eller ændres.

3.4.2 Netværk

Telefonen er opsat til skolens trådløse netværk.

3.4.3 Mail

Til brug for arbejdsmail, er Outlook App installeret. Den indbyggede mail må gerne anvendes til privat mail, men ikke arbejdsmail. Maildata må ikke forlade EU-området. Se pkt. 3.5.6.

3.4.4 APP's

Du må gerne installere sikre[2] APP's og benytte den til betalingsmiddel.

3.4.5 SMS-donationer

Du må ikke sende SMS-donationer, da CB står som betaler.

[2] APP's der ikke har dårligt renomé (som mange kinesiske App's har) og visse spil.

3.4.6 Bortkomst

Hvis du mister din telefon, skal du melde det. Når IT-administrationen får besked, kan telefonen spores og evt. spærres.

3.5 Personoplysninger

”Personoplysninger er enhver form for information om en identificeret eller identificerbar person.”

Det kan være alt fra navn, skostørrelse, adresse, karakterer osv.

Personoplysninger skal behandles jf. ”Persondataforordningen” (GDPR). GDPR har til formål at beskytte data generelt, og den enkelte EU-borgers data.

3.5.1 Personfølsomme oplysninger

Personfølsomme oplysninger, er en særlig kategori af personoplysninger, som kræver særlig beskyttet behandling. Det drejer sig om:

- Race eller etnisk oprindelse
- Politisk, religiøs eller filosofisk overbevisning
- Fagforeningsmæssige tilhørsforhold
- Genetiske data (DNA)
- Biometriske data med formål at foretage identifikation
- Helbredsoplysninger
- Seksuelt tilhørsforhold
- Oplysninger om strafbare forhold – herunder børneattest

3.5.2 Samtykkeerklæring

Skal udfyldes inden:

- Opbevaring af Personfølsomme data.
- Offentliggørelse af billeder og videoer.

Det er legitimt, at trække en erklæring tilbage.

3.5.3 Dataoplysning

Alle der måtte ønsker det, kan få udleveret de oplysninger, de er registreret med.

3.5.4 Dataajourføring

Oplysninger skal holdes ajour, og rettes ved konstatering eller henvendelse.

3.5.5 Dataminimering

Data må kun opbevares så længe der er behov for dem. Ansatte og elever der stopper, skal slettes.

3.5.6 Opbevaring af data

Persondata må ikke opbevares uden for EU.

Det betyder, at kun godkendte sky-tjenester (mail, filer og videomøder) må benyttes. Eneste godkendte, er Microsoft.

DropBox, iCloud, FaceBook, Amazon, Google m.fl. må ikke anvendes til persondata.

3.5.7 System- og programgodkendelse

Systemer og programmer der behandler personoplysninger, skal risici-vurderes i forhold til, hvordan personoplysningerne behandles. Proceduren hedder DPIA (Data Protection Impact Assessment).

3.6 Godkendte systemer og programmer

Kun godkendte systemer og programmer må anvendes. En liste kan ses på:
https://it.cabh.dk/Home/Indhold/105

3.6.1 Godkendelse af nye systemer og programmer

Ønskes et system eller program godkendt, kontaktes IT-administrationen i første omgang. Ud over DPIA, vil almindelig funktionalitet og evt. kendte sikkerhedsbrister blive vurderet, og om nødvendigheden af anvendelse i forhold til måske allerede godkendte system/program. Det anses ikke for rimeligt, at studerende skal beherske 4 – 5 forskellige videokonfrerencesystemer.

3.7 Internettet

3.7.1 Mailsystemet

Mailtrafik der passerer gennem internettet, er ikke sikker!

- Intern mail ER sikker (og til de andre skoler under EFIF), men pas på, når der sendes "ud af huset" (til eksterne adressater).
- Ekstern mail er IKKE sikker, og meddelelser med CPR og personfølsomme oplysninger SKAL krypteres.

Undgå i øvrigt at have følsomme oplysninger liggende i mailsystemet. Du kan ved en fejl komme til at sende til uautoriserede modtagere.

3.7.1.1 Farlige mails

Kriminelles 1.-prioritet til at trænge ind i systemer, sker via mails. Det er desværre rigtigt nemt at sætte en anden afsender på, end dén det faktisk er. Ved at få mail'en til at se officiel ud, kan man blive snydt til at gøre dét de ønsker.

3.7.1.2 Sikker afsendelse & modtagelse

Til afsendelse anvendes IMS Digital Post.

Til modtagelse anvendes Medarbejdersignatur i Outlook-klienten.

3.7.2 Kriminelles virksomhed

Kriminelles foretrukne metode til at trænge ind i systemer, sker ved at snyde virksomhedens medarbejdere. *Det er desværre en meget effektiv metode.*

De anvender følgende fremgangsmåder:

3.7.2.1 Phishing

Kriminelle snyder dig til at udlevere oplysninger eller gøre ting.

Eksempel:	Løsning:
Du er regnskabsmedarbejder, og 23. december modtager du en mail fra Direktøren om, at der – inden året er omme – skal indbetales honorar for et anvendt rekrutteringsbureau. Navnet er kendt, og der oplyses kontonummer. Du er alene tilbage, for alle er gået på juleferie.	Vær meget forsigtig med at overføre beløb ved en foranstående helligdags-/ferieperiode. Transaktionen er svær at stoppe fordi den foregår elektronisk – og bankpersonalet har også ferie. Ring til Direktøren for bekræftelse.
Du modtager en mail fra Visa, der siger at der er problemer med en betaling. De kan oplyse de første 4 cifre i kortnummeret, og beder dig om udløbsdato og kontrol-kode.	Udlever aldrig kreditkortoplysninger!

Du bliver ringet op af Microsoft, der meddeler, at din computer bliver brugt i et koordineret angreb mod Det Hvide Hus. De vil gerne have adgang til din computer, så de kan fjerne den skadelige software.	”Som om Microsoft ringer til dig!” Stol aldrig på sådanne opkald. Det er nu, der vil blive installeret skadelig software. Læg røret på, og meld episoden.

3.7.2.2 Ransomware

Ransomware er en skadelig software (orm), der krypterer alle filer på det lokale netværk. Ormen starter med backup'en, derefter serverne, og til sidst computerne. Nu kan virksomheden ikke længere anvende sine IT-systemer og oplysninger.

De kriminelle efterlader en besked om, hvordan filerne kan dekrypteres – men kun mod betaling af en meget stor sum penge (i kryptovaluta).

Mange – både meget store, men også små – virksomheder bliver ramt af dette i øjeblikket, og risikoen for at blive ramt, er virkelig stor. Eneste redning for virksomheden, når det sker, er en valid backup.

De kriminelles metode er, fx at fremstille en mail med et officielt udseende, der får modtageren til at klikke på et link, hvorefter den skadelig software installeres.

Eksempel:	Løsning:
Du modtager en mail fra GLS, der meddeler, at din forsendelse er forsinket, men at du kan tracke din forsendelse via dette link. Da du klikker på det, beder Windows dig om tilladelse til at foretage en handling.	Dette er sidste advarsel inden der bliver installeret skadelig software. Afbryd handlingen. Sluk evt. computeren på den hårde måde (hold tænd-/sluk-knappen nede i mere end 20 sekunder. Vigtigt! Hvis det alligevel sker for dig, så meld omgående (ring) til IT, så ulykken kan standses.

Den skadelige software ligger overalt på internettet og venter kun på at blive aktiveret. Det er altså ikke et målrettet angreb – det fungerer mere som en landmine, der venter på, at blive trådt på.

3.7.2.3 Malware

Malware er al anden uønsket software der bliver installeret med henblik på reklamer (spam) eller omdirigering til særlige hjemmesider.

3.7.3 Videomøder

Teams og Skype er godkendt – øvrige er ikke (Zoom, Discord, Google Duo, Facebook, Messenger, Whereby).

De øvrige tjenester virker godt, og er gratis. Andre virksomheder anvender dem måske derfor, og man kan være tvunget til at deltage i et møde vha. disse. Hvis det ikke kan undgås at skulle anvende ikke-godkendte tjenester, så gør det med bevidstheden om, at systemerne ikke er sikre.

3.8 Fysisk beskyttelse

3.8.1 Offentlige rum

Hvis du har arbejdsplads i et offentligt område, er din computer ekstra udsat. Der kan fx blive isat en USB-pen, der kan lave alt muligt skadeligt – lige fra Ransomware til et ”Keylogger-program” der optager alt hvad du taster (og derved aflure dine passwords).

3.8.2 Lås nede

Lås vigtigt/sensitivt materiale nede. Især hvis du deler lokale med andre.

Visse materialer kræver godkendte opbevaringsmidler.

3.8.3 Lås lokalet

Sørg for at låse lokalet af, når du er den sidste der forlader det – også selvom det er kortvarigt.

3.8.4 Destruering

Smid ikke bare ting i skraldespanden – du ved ikke hvor det havner.

- Sensitive dokumenter (fx med CPR-numre) skal makuleres. Makulatorer er opsat i alle kopirum.
- Databærende medier (fx harddiske, USB-penne, DVD'ere m.fl.) skal ødelægges.

4 De 10 bud

1. Skift dit password ofte
2. Lås din skærm når du går
3. Vær kritisk med at åbne links
4. Hav ikke persondata på din PC
5. Samtykke ved foto/video
6. Persondata kun med sikker mail
7. Persondata kun på netdrev/ADM sys
8. Tænk, inden persondata deles
9. Papirer låses nede og makuleres
10. Tvivl? Spørg kollega, leder eller IT