OKT 2024

GRUNDLÆGGENDE IT OG CYBERSIKKERHED - KAN ANVENDES TIL PRIVAT BRUG

01000111 01010010 01010101 01001110 01000100 01001100 11000011
10000110 01000111 01000111 01000101 01001110 01000100 01000101
00100000 01001001 01010100 00100000 01001111 01000111 00100000
01000011 01011001 01000010 01000101 01010010 01010011 01001001
01001011 01001011 01000101 01010010 01001000 01000101 01000100
00100000 00001010 00001010

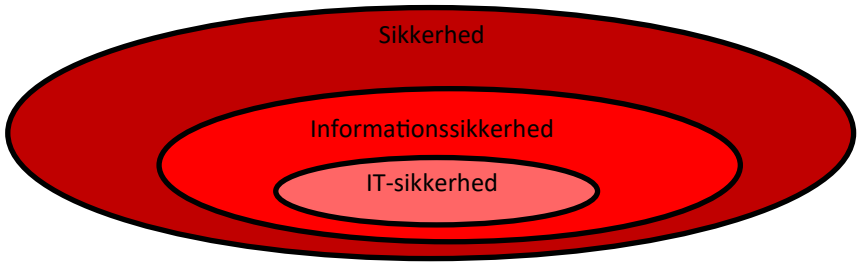
TRUSLEN MOD BORGERE og DANMARK	
Cyberspionage	Meget høj
Cyberkriminalitet	Meget høj
Cyberaktivisme	Høj
Destruktive angreb	Lav
Cyberterror	Ingen

De 6 gode råd

1. Opdater altid din computer og programmer. ALTID!
2. Klik ikke på nogen links eller filer → Er du i tvivl, er du ikke i tvivl.
3. Lav password på mindst 12 karakterer uden personlige ord og brug 2-faktor.
4. Brug ikke USB udstyr du ikke kender.
5. Slå wifi og Bluetooth fra når det ikke anvendes, samt brug ikke offentlige netværk (brug evt. VPN).
6. Hav en offline backup af dine vigtige filer (gem aldrig dit arbejde på skrivebordet).

Hvad er informationssikkerhed?

Informationssikkerhed er de samlede foranstaltninger, hvor IT-sikkerhed, cybersikkerhed, datasikkerhed osv. er en del af informationssikkerhed.



GODE RÅD TIL HJEMMET OG ARBEJDET

Symptomer på MALWARE:

- Forøget brug af CPU kraft.
- Dit device er langsommere end normalt.
- Dit device fryser ofte eller går i sort.
- Du kan browse langsommere på nettet.
- Mærkelige / uforklarlige problemer med dit netværk.
- Filer er modificeret eller mangler.
- Du får måske ukendte filer, programmer eller ikoner.
- Programmer ændrer sig selv, eller slukker.
- E-mail sendes uden din viden.
- Programmer åbner pludseligt.

Eller det modsatte af alt ovenstående.

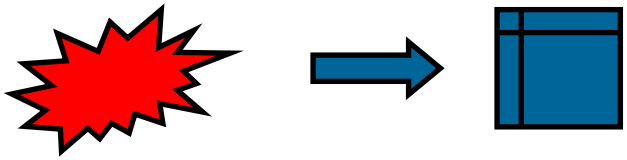
VED TYDELIGE TEGN PÅ MALWARE SLUK IKKE pc, MEN TRÆK NETVÆRKSSTIKKET UD / SLUK WIFI.

Rapportering / Melding om uregelmæssigheder:

Ved uregelmæssigheder / kompromittering skal følgende underrettes

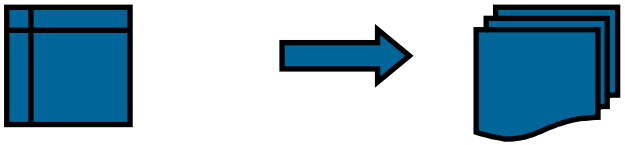
Trin 1: Nærmeste leder / chef

Trin 2: Indberetning til IT– og Digitalisering
”Indberet I-Sikkerhedshændelse” på Vicky/selvbetjening
Indberet i-sikkerhedshændelse - Vicki - Viborg Intranet



1. melding fra bruger.
Skal ske inden for timer/min.

IT– og Digitalisering
Reagerer hurtigst muligt på henvendelse



Eventuelt 2. melding fra bruger
Skal ske hvis ny info. dukker op

IT– og Digitalisering
Reagerer opdater hændelseslog

Værktøj	Beskrivelse	Link
Diverse værktøjer:		
Have I been pwnd	Har en given mail været kompromitteret. F.eks. i forbindelse med et læk eller hack af en hjemmeside.	Haveibeenpwnd.com
Advanced googeling	Anvendelse af de avancerede googlesøgninger. Få mere ud af google og gør søgningermere målrettet	Google.com/ advanced_search
Who Is	Få oplysninger om ejeren af et website	Whois-search.com
Ukendt num-mer	Tlf.nr der er kendt som SCAM	ukendtnummer.dk
Midlertidig mail		
10 minute mail	Midlertidig mail der kun virker i 10 min	10minutemail.com/
Kontroller links		
Virus total Scamadviser	Kontroller et link eller en fil Kontroller et link	virustotal.com Scamadviser.com
Find metadata i billeder (exif)		
MetaData	Find metadata i en fil	metadata2go.com
Gode informationssider til den nysgerrige		
IT-borger	Offentlig side med mange gode råd om sikkerhed.	it-borger.dk
Sikker Digital	Infoside med gode råd og vejledninger.	sikkerdigital.dk
GDPR	GDPR forklaret på 5 min.	gdpr.dk
CFCS	Center for Cybersikkerhed	cfcs.dk

GODE RÅD TIL HJEMMET OG ARBEJDET

Generelle råd:

- Hold din computer og programmer opdateret. ALTID!
- Kontroller et link hvis du er i tvivl..
- Vælg "offentligt netværk" når du kobler på et nyt netværk.
  - Så har PC'en højere beskyttelses niveau
- Hav gerne to mailkonti, En til det officielle og en til det andet andet
  - Undgå at bruge din "officielle" mail til det hele
- Gør dig selv til bruger på computeren (ikke admin).
- Sørg for at have en offline backup.
- Krypter HDD på din PC (f.eks. bitlocker)

Mobile enheder (devices):

- Vær skeptisk hvis din telefon går på 2G (Edge).
- Slå Bluetooth og WIFI fra når du ikke bruger det.
- Pas på phishing via SMS/MMS, sociale medier osv. Kontroller link.
- Installer antivirus på din enhed og vær skeptisk når du henter APP 's.
- Begræns dine APP 's adgang til mikrofon, kamera, lokaliteter, billeder,
- kontakter osv. (Læs betingelserne).
- Brug kun din egen lader til mobilen.
- Slå Siri, google assist osv. fra.
- Tildæk eller deaktiver WebCam.
- Spørg dig selv: "Hvad har min mobil set og hørt i dag?"

De 6 gode password-råd:

1. Minimum 12 karakterer (gerne flere)
2. Brug ikke personlige ord
3. Skift det jævnligt (mindst hver 180 dage)
4. Genanvende ikke passwords
5. Brug to-faktor (multi-factor)
6. Brug en password manager til at huske dem— gem ikke i browseren
   - Fx E-boks kodehusker, Bitwarden, Authy, Dashlane

USB enheder:

- Anvend aldrig USB enheder du ikke kender.
  Finder du et USB, så aflever det til Service Desk eller din leder
- Krypter dine USB enheder (BITLOCKER).
- Afmærk dine USB enheder.
- Anvend aldrig billig USB enheder fra f.eks. Wish, ebay osv.
- Anvend ALDRIG private USB enheder i tjenstlig udstyr... og omvendt!
- Gælder også opladning af mobiltelefon

GODE RÅD TIL HJEMMET OG ARBEJDET

Ransomware:

- Betal aldrig løsesummen
- Hold alt opdateret (også APP 's).
- Hav ikke "kompromitterende" eller belastende data liggende på online maskiner.
- Lav jævnligt en offline backup → F.eks. ekstern HDD (også fra data i
- skyen).
- Lad ikke data "samle støv' → læg dem på en backup.

Sikker browsing:

- Hold dine browsere opdaterede.
- Lad aldrig browseren huske dine koder, kortoplysninger etc.
- Tilføj en ADD-Blocker i browseren (Tilføjelsesprogram).
- Indtast kun oplysninger på sider du har tillid til og som er (HTTPS)
- Tilføj Add-ons til din browser. Feks:
  - ◊ AddBlock — Fjerner pop-up reklamer
  - ◊ Ghostery — Fjerner trackere
  - ◊ Defender sikker browsing — Beskyt mod ondsindede links
  - ◊ HTTPS Everywhere - Fra HTTP til HTTPS
  - ◊ Click&Clean — Fjern historik m.m.
- Anvend evt. browseren "BRAVE".

Trådløse tilkoblinger:

- Slå Wifi og/eller bluetooth fra når det ikke anvendes.
- Anvend ikke offentlig WiFi (bus, hotel, MC-D osv.)
- Beskyt dine kreditkort med RFID sikker pung, lomme eller lignende.

Social Engineering:

- Vær skeptisk i mærkelige situationer (f.eks. opkald).
- Er du i tvivl om rigtigheden, valider informationen fra andet sted.
- Oplys aldrig personlige oplysninger på alm. mail eller telefon.
- Makuler personfølsomt / klassificeret affald.
- Intet er gratis, så vær skeptisk hvis en ydelse præsenteres som gratis.
- Vær opmærksom ved trusler eller deadline/nedtælling.

GODE RÅD TIL HJEMMET OG ARBEJDET

Sociale medier:

- Vær kritisk mht. de informationer du lægger op.
- Kan det tåle at stå på en plakat et offentligt sted?
- Kan det give et større billede af dig, når det kombineredes med alt det andet du deler?
- Begræns de personlige informationer du deler.
- Undgå at lægge oplysninger op der viser din relation til FSV.
- Læg ikke billeder op der viser personer, materiel, indretning af kaserner/ lejre osv.
- Anvend sikkerhedsindstillinger (begræns din profil).
- Accepter kun venner du kender i virkeligheden.
- Vær skeptisk når du møder en på nettet.
- Brug ikke din socialmedie-konto til at logge ind andre steder (f.eks.
- Facebook til at logge ind på Microsoft osv.).
- "Google" dig selv, eller få en anden til det. Reager på det du ikke er bekendt med.

Internet of Things (IOT):

- Skift altid standard password.
- Anvend ikke billigt udstyr købt på f.eks. ebay m.m.
- Lav separate WIFI netværk til smart TV, køleskab osv. , eller tag internetstikket ud af udstyret når det ikke anvendes.
- Skift opsætning på din Wifi router:
  - ⇒ Disable adgang til router fra internettet.
  - ⇒ Ændre standart kodeord + bruger til router.
  - ⇒ Ændre netværksnavn (SSID) (unikt navn til et WLAN)
  - ⇒ Skift password til Wifi
- På samme måde skift standardindstillinger på dine IOT devices.

Kommunens udstyr:

- Når man forlader sine enheder både i hjemmet og på arbejdet, skal udstyret låses.
- Overførsel mellem kommunens udstyr og til privat udstyr er ikke tilladt.
- Hver opmærksom på, at alt telefoni i princippet kan aflyttes .
- Alt IT materiel skal markeres med mærkat fra Viborg Kommune (PC, Printer, iPads osv).
- Hjemmearbejdes computer skal enten være i personlig varetægt eller opbevares som værdigenstand i aflåst skab/taske (som pung eller lignende).
- Personfølsomme arbejdsdokumenter på hjemmearbejdspladsen skal enten være i personlig varetægt eller opbevares som værdigenstand i et aflåst skab/taske
- Alle har et ansvar for informationssikkerheden overholdes.