Cybersikkerhed og gode digitale vaner

I anledning af national cybersikkerhedsmåned

Nyit.dk og Digital Fighters

Hvem er Digital Fighters Aps

- Uvildig IT-rådgiver med over 30 års erfaring
- Ekspertise indenfor digitalisering og IT-sikkerhed
- Fokus på:
  - IT-sikkerhed
    - Undervisning for bestyrelse og ledelse
    - Udarbejdelses af D-mærket, sikkerhedspolitikker, beredskabsplaner
    - Awareness træning for medarbejdere
  - Digitalisering
    - Undervisning for bestyrelse og ledelse
    - Digitaliseringsforløb for virksomheder

Trusselsbilledet er ændret

- Der er kommet betydeligt flere hacker- og phishing-angreb, næsten en tredobling.
- Fokus er flyttet fra store virksomheder til mindre virksomheder
- 26% af danske virksomheder melder at de har været udsat for sikkerhedsbrud.

De 7 gode råd om IT-sikkerhed

1. Få overblik over vigtige data og systemer
2. Opdater programmer løbende
3. Køb antivirus og firewall
4. Tag backup af data
5. Lær at spotte mistænkelige mails
6. Lav stærke adgangskoder og brug to-faktor login
7. Stil sikkerhedskrav til IT-leverandøren

1. Få overblik over vigtige data og systemer

- Kortlægning af virksomhedens data, systemer og kritiske processer
- Prioritering og vurdering af følsomhed
- Beredskabsplan og nødplan
- Periodisk opfølgning

2. Opdater programmer løbende

- Anvende nyeste versioner hvor muligt
- Automatisk opdatering
- Prioriteret plan for at opdatere forældede systemer
- Overvej cloud eller købe nyt

3. Køb antivirus og firewall

- Sikre at virksomhedens udstyr er beskyttet med effektiv og opdateret antivirus
- Antivirus er i dag avancerede systemer med endpoint protection

4. Tag backup af data

- Backup, backup, backup…
- Absolut vigtigste IT-sikkerhedsøvelse. Når ALT går galt har vi kun backup'en at falde tilbage på.
- Overvej flere versioner og typer af backup
- Test at genetablering rent faktiske kan lade sig gøre!
- Hvor lang tid vil det tage?

5. Lær at spotte mistænkelige mails

- Få gode digitale vaner, opbyg en IT-sikkerhedskultur
- Lav awareness træning for medarbejdere
- Gælder også SMS
- Lær de 7 tegn på phishing
- Brug ”Mit digitale selvforsvar” app’en

De 7 tegn på phishing

1. Afsender e-mail adressen er ikke fra den organisation den udgiver sig for at være.
2. Er der links eller vedhæftede filer?
3. Budskaber er ikke målrettet dig?
4. Er mailen dårligt skrevet, stavefejl?
5. Bedes der om følsomme oplysninger?
6. Er der et element af hastværk? Skal vi skynde os?
7. Lyder det for godt til at være sandt?

Hvad gør jeg når jeg bliver ramt?

1. Tag gerne et billede af det du oplever?
2. Sluk enheden
3. Kontakt IT-afdelingen eller din IT-leverandør

6. Lav stærke adgangskoder og brug to-faktor login

- Anvend to-faktor login hvor muligt
- Genanvend aldrig passwords
- Brug en password manager fx Keeper, Nordpass eller 1password.

7. Stil sikkerhedskrav til IT-leverandøren

- De fleste virksomheder outsourcer hele eller dele af deres IT til leverandører.
- Hvad gør IT-leverandøren for at beskytte mod uønsket adgang?
- Hvad gør IT-leverandøren for at sikre tilgængelighed og høj oppetid?
- Hvad er opgavefordelingen mellem jer som kunde og IT-leverandøren?
- Hvad er **deres** beredskabsplan?
- Er jeres krav nedfældet i en kontrakt?

Overvej at blive D-mærket

- D-mærket er Danmarks nye mærkningsordning for it-sikkerhed og ansvarlig dataanvendelse
- D-mærket tydeliggør hvilke virksomheder, der udviser digital ansvarlighed og giver dermed både forretningsværdi til virksomhederne, tryghed til forbrugere og kunder og skaber et stærkere digitalt Danmark.

digital tryghed

IT Managed Service Provider

”IT-Infrastruktur er alle de komponenter der bærer virksomhedens IT løsning, dvs. Servere, Cloud, Netværk, PC’er, printere, sikkerhed og basis software såsom Windows, Office og lign.
Managed Service Provider forkortes; MSP, hvilket vil sige at vi tilbyder løsninger der er administreret og monitoreret af os, således at vi tager ansvaret for IT-Infrastruktur løsningen og holder den stabilt og sikkert kørende!

Med andre ord er vi Jeres ”IT afdeling on-demand”

nyit.dk

- Making IT work

Kort om os

- Startet i 2008
- 6 ansatte
- Faguddannet og certificerede i flere IT fagområder
- Arbejder ud fra anerkendte procedurer og best practices
- Mange års erfaring fra bl.a. Danfoss, ECCO og IP Nordic

- Fokus alene på erhverv og frie skoler

nyit.dk

Microsoft Silver Partner · Acronis · Acronis Authorized Partner · Hewlett Packard Enterprise · Lenovo Business Partner · UEWA Ubiquiti Enterprise Wireless Admin

- Making IT work!

Agenda

- IT sikkerhed i et helikopterperspektiv
- Cybertruslen lige nu
- Casestorys
- Hvad kan man så gøre?

- Making IT work!

Forord

- IT-sikkerhed er et meget bredt emne og består af rigtig mange elementer og lag.
- Hvert element eller hvert lag, kan i princippet blive til et kursus for sig selv og nogle ville strække sig over flere dage, så i dette korte seminar, når vi ikke at gå i dybden, vi har udvalgt de områder der er typiske og hvad man typisk kan gøre for at sikre sig.
- I behøver ikke tage noter, vi sender både præsentation og et link til en video af seminaret.
- Har i spørgsmål, så er de velkomne, men vi har ikke meget tid, så er de for tidskrævende, så kan vi tage dem efter seminaret.

IT sikkerhed, set fra oven

- **IT-sikkerhed** er i dag på mange måder både blevet væsentligt mere komplekst og væsentligt mere simpelt end tidligere.

- **Komplekst;** fordi der findes rigtigt mange forskellige angrebsvektorer i et moderne IT landskab, og det derfor kan være svært at følge med i den konstante udvikling, ikke mindst set ud fra et IT sikkerheds perspektiv

- **Simpelt;** Fordi alle der sidder herinde i dag på 10 minutter kunne købe sig til en fuldt automatiseret og køreklar løsning, og dermed angribe 100, 100.000 eller 10 millioner brugere på samme tid - alt sammen til den nette pris á 10 dollar!

- Making IT work!

Live trusselsbillede

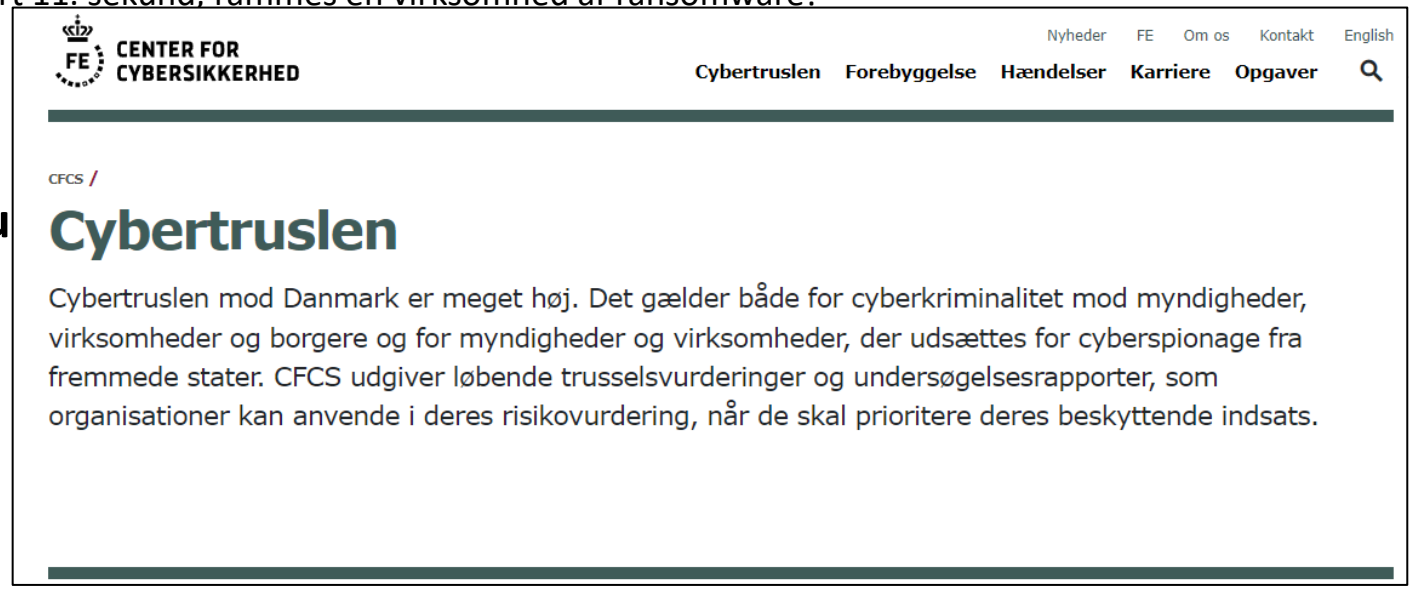
Vi skal tage et kort kig på hvordan nogle forskellige trusselsbilleder tager sig ud live, blot for at illustrerer hvor vanvittigt trusselbilledet reelt er.

https://cybermap.kaspersky.com/
https://livethreatmap.radware.com/

Hvert 11. sekund, rammes en virksomhed af ransomware!

De **lle udsnit af hele billedet!**

Tru



- Making IT work!

Vidste du at..

- 60% af de små virksomheder, der har været udsa[illegible]ccesfuldt cyberangreb er gået konkurs efter seks måneder
- 31% af de store virksomheder (250+) har oplev[illegible] 2019, dette er siden steget med gennemsnitl[illegible]
- 70% af målrettet cyberangreb forbliver uop[illegible] 205 dage at opdage de resterende 30%!
- 1 ud af 4 SMV´er har ikke implementeret essentielle sik[illegible] backup og software opdatering!

Få det nu fixet....

* Data indhentet fra Danmarks statistik, systemgruppen, IBM, CSIS og Sikkerdigital.

- Making IT work!

Casestory

- Mange virksomheder ønsker ikke at stå frem, når de er blevet ramt, simpelthen fordi det går ud over deres brand og troværdighed!

- Vi skulle have haft besøg af en *regionschef for Skandinavien* fra en stor international koncern, men han fik desværre mundkurv på i sidste øjeblik!

- Vi vil i stedet, anonymiseret, fortælle om et par virkelige hændelser her i området.

- Flere casestories kan ses på https://sikkerdigital.dk/virksomhed/virksomhedscases

Casestory

- Enkeltmandsfirma
- Mailkonto kompromitteret – altså havde andre blot fået adgang dertil
- *Hackere* opsnappede de korrekte regninger, og ændrede disse med forkerte kontooplysninger.
  Regningerne blev efterfølgende sendt til kunderne.
- Kunderne betalte således regningerne til hackerne og ikke til virksomheden
- +250.000 kr. gik tabt inden kunden opdagede hvad der skete!
- Meget subtil måde at berige sig på – der kan gå lang tid inden man opdager hvad der er sket, og kan reagere.

✓ Løsningen var at implementere MFA

Casestory

- Større koncern i Sydjylland
- Store dele af infrastruktur kompromitteret af *hackere* fra Rusland
- Koncernen ude af stand til at arbejde, producere varer eller købe og sælge – ingen ordre ind eller ud
- Kompromitteret ca. 2 år forinden, hackere rekognoscerede i netværket via en ”glemt” terminalserver med adgang udefra (ren bruteforce)
- Adgang til sidst solgt til 3. part, som valgte at aktivere en kryptering (ransomware) af hele it infrastrukturen

✓ Gennemgå og fjerne firewall/remote adgang for uvedkommende
✓ Opdatere sikkerhedssoftware, køre scan
✓ Reetablere fra backup

- Koncernen var mere eller mindre ude af drift i godt 3 uger
- Virksomheden led datatab, der er dog ikke opgjort et omfang.
- Alvorlige økonomiske konsekvenser, vi er dog ikke bekendt med det reelle omfang, men helt sikkert på den forkerte side af en million.

- Making IT work!

Hvad kan man så gøre?

Overordnet set er der følgende indsatsområder:

- Uddan og træn jeres medarbejdere / Awareness
  - IT sikkerhedspolitik → Digital Fighters ApS
  - Shadow IT
  - CEO Fraud
  - Fysiske faktorer / Human errors
  - Insider Threat
- Beskyt dine virksomhedsdata
  - Domæne og DNS sikkerhed
  - Cloud sikkerhed, antispam, logins, MFA
  - Netværkssikkerhed, firewall, switche, wifi
  - Lokal sikkerhed, logins, pc, server, antivirus, antiransomware, BitLocker.
- Opdater ALT
  - Herunder software, hardware, computere, smartdevices, netværksudstyr osv.
- Backup
  - Backup er det første du bør få styr på og forhåbentligt din sidste redning!

- Making IT work!

Uddan og træn jeres medarbejdere

- Mennesket er nysgerrigt af natur
- Mennesket søger løsninger på problemer
- Den stressede hverdag buldrer derud af
- Alle mennesker begår fejl

Vidste du at:

- 9 ud af 10 sikkerhedsbrud kan spores tilbage til brugeren foran computeren
- 8% af medarbejdere i en given virksomhed, giver deres login eller anden virksomhedsdata væk til fremmede i god tro…

Derfor:

✓ Læg en plan for awareness og uddannelse af jeres brugere, det kan være helt simple IT regler der informeres om ved ansættelse eller ved konkrete kurser.

Shadow IT

- Når brugerne ikke får stillet de værktøjer til rådighed som de har behov for, så finder de selv en løsning.
- Disse værktøjer kan i mange tilfælde være fyldt med spyware eller i endnu værre tilfælde, give uvedkommende adgang gennem bagdøre.
- Ofte er disse værktøjer også brugt i strid med licensbetingelserne.

Løsning:

✓ Sørg for at brugerne har de rigtige værktøjer, som er godkendt af IT-afd./IT Leverandør
✓ Sørg for at brugere ikke er lokal administrator

CEO Fraud

- Beder din chef dig på mail om at købe en vare eller overføre et større beløb til en ukendt konto – gerne hurtigst muligt, ellers går virksomheden glip af en kæmpe handel?
- Kaj har allerede nævnt dette i sin præsentation - tjek bla. mailheader, tjek sproget (ligner det, at det kommer fra chefen?), ville chefen overhovedet sende en mail og spørge om dette?
- Chefens mailkonto KAN være kompromitteret, så du kan risikerer at mailen reelt kommer fra chefens mailkonto…

Vær skeptisk:

✓ Ring til chefen og bed vedkommende konfirmere – ikke på SMS (kan spoofes relativt nemt..!)
Hvis du ikke kan få fat på hende, så må det vente indtil hun reagerer med et verificeret opkald!

Fysiske faktorer / Human errors

- Fysisk adgang til virksomhedens IT systemer
  Hvem har adgang til f.eks. serverrummet/krydsfelter, eller hvem ved hvor nøglen er – hænger den måske ved siden af døren?
  Eller kan fremmede måske komme direkte ind fra gaden og sætte sig ved et skrivebord ved siden af et netværksstik?
- Eller hvad med et USB drev du tilfældigt finder på parkeringspladsen?
- Hvad med rengøring, der typisk kommer sent om aftenen/natten, og typisk har adgang til alt med en A-nøgle?
- Har alle ansatte adgang til alt på filserveren?

✓ Adgangskontrol – kort/kode. Overvågning er fin, men er reaktivt…
✓ Brug ALDRIG en ”fundet” USB – bare det at smide den i computeren kan være nok til at starte et angreb. Giv den i stedet til jeres IT folk, og lad dem undersøge den.
✓ Begræns adgang til specifikke rum – rengøring behøver ikke have adgang til serverrum uden opsyn
✓ Begræns brugernes adgange til filer/drev – hvis de ikke har adgang kan de heller ikke ”komme til” at slette noget ved et uheld eller ved overlæg.
✓ Backup!

Insider Threat

- Insider threat – En opsagt og sur medarbejder er nemmere at lokke til at foretage angreb på virksomhedens IT.
  Eller en måske en medarbejder som privat er økonomisk udfordret, og kan lokkes med pengebeløb mod at udføre en lille handling på sin computer?
- En opsagt medarbejder kan i vrede sende usande e-mails eller slette filer eller på anden måde forvolde skade.
- Eller via trusler: ”Vi ved hvor du bor og hvad dine børn hedder…” Påvirkning af en ansat som derved tvinges til at foretage visse ting internt i virksomheden.

✓ Sørg for at i har en procedure ved opsigelse, således at vedkommende ikke har adgang til it systemer efter selve opsigelsessamtalen.
✓ Adviser IT afdelingen i god tid, så de kan lukke adgang i rette tid – typisk under selve samtalen.
✓ Sørg for at medarbejdere aldrig har adgang til mere end absolut nødvendigt.

Hvad kan man så gøre?

Overordnet set er der følgende indsatsområder:

- Uddan og træn jeres medarbejdere / Awareness
  - IT sikkerhedspolitik → Digital Fighters ApS
  - Shadow IT
  - CEO Fraud
  - Fysiske faktorer / Human errors
  - Insider Threat

- Beskyt dine virksomhedsdata
  - Domæne og DNS sikkerhed
  - Cloud sikkerhed, antispam, logins, MFA
  - Netværkssikkerhed, firewall, switche, wifi
  - Lokal sikkerhed, logins, pc, server, antivirus, antiransomware, antiPhishing, threat control, BitLocker.

- Opdater ALT
  - Herunder software, hardware, computere, smartdevices, netværksudstyr osv.

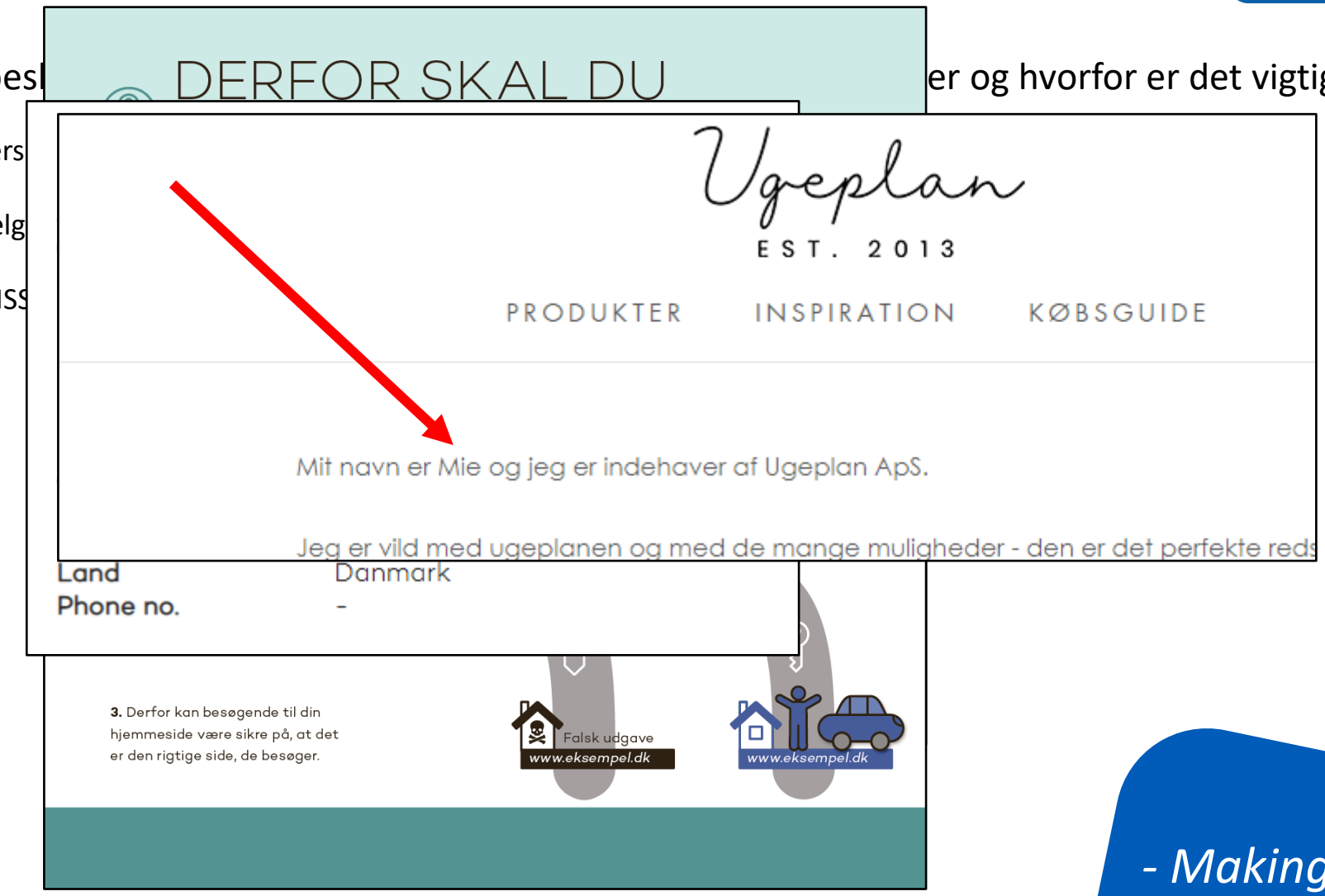
- Backup
  - Backup er det første du bør få styr på og forhåbentligt din sidste redning!

- Making IT work!

Domæne, WEB og DNS

Hvordan besl er og hvorfor er det vigtigt?

- ✓ Ejers
- ✓ Vælg
- ✓ DNSS



- Making IT work!

Cloudsikkerhed

- Idet cloud er blevet allemandseje i dag, følger der også et behov for øget sikkerhed herpå.
- Som udgangspunkt kan du prøve et uendeligt antal gange at logge ind på din cloudkonto – det kan alle andre dermed også.

✓ Derfor er MFA et must.

✓ Hvis det blot er et spørgsmål om at beskytte en enkelt cloud konto eller 2, så er Microsofts egen MFA ganske udmærket, denne kan nemt aktiveres via portal.office.com

✓ Så snart i stiller andre krav til MFA (lokale logins på computere, server login, VPN osv.) så slår den ikke til længere, her bør man søge et 3. parts alternativ – DUO Security er et rigtig godt bud.

Cloudsikkerhed

	Only	Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	1 sec	5 secs
7	Instantly	Instantly	25 secs	1 min	6 mins
8	Instantly	5 secs	22 mins	1 hour	8 hours
9	Instantly	2 mins	19 hours	3 days	3 weeks
10	Instantly	58 mins	1 month	7 months	5 years
11	2 secs	1 day	5 years	41 years	
12	25 secs	3 weeks	300 years	2k years	
13	4 mins	1 year	16k years	100k years	
14	41 mins	51 years	800k years	9m years	200m years
15	6 hours	1k years	43m years	600m years	15 bn years
16	2 days	34k years	2bn years	37bn years	1tn years
17	4 weeks	800k years	100bn years	2tn years	93tn years
18	9 months	23m years	6tn years	100 tn years	7qd years

34k years

TIME IT TAKES A HACKER TO BRUTE FORCE YOUR PASSWORD

HIVE SYSTEMS

-Data sourced from HowSec

net

- Making IT work!

Netværkssikkerhed

Overordnet

- ✓ Least privilege – sørg for at man som udgangspunkt har så få rettigheder som muligt

Udstyrsvalg

- ✓ Next-gen Firewall (application awareness and control, integrated intrusion prevention, and cloud-delivered threat intelligence.)
- ✓ Cloud managed og monitored
- ✓ Cisco / Meraki, FortiGate, Ubiquiti mf.

Logisk sikkerhed

- ✓ VLAN segmentering
- ✓ Firewall regler
- ✓ GEO Filtrering
- ✓ WIFI sikkerhed - Gæstenetværk

Lokal sikkerhed

Overordnet

- Sidst bastion – jeres interne IT infrastruktur

Antivirus - AntiX

- ✓ Next-gen Antivirus
  - ✓ ATC/Antiransomware
  - ✓ Sandboxing
  - ✓ EDR
- ✓ Cloud managed og monitoreret
- ✓ Anti-malware og -spam på mailtrafik er essentielt til at opretholde et stærkt sikkerhedsninveau

Login/lokal sikkerhed

- ✓ MFA på lokale computere/servere – forhindrer at uvedkommende med kompromitteret brugernavn/password har adgang, selvom de står foran maskinen
- ✓ Bitlocker på alle maskiner – forhindrer at data kan læses af uvedkommende, også selvom de har taget maskinen med under armen.
  Bitlocker nøgler bør kunne gemmes et centralt sted – IKKE på et stykke papir eller en fil på filserveren.
  Hvorfor Bitlocker?
  Tyveri af IT udstyr, der er let omsætteligt er stadigt et stort problem – det samme gælder for glemsomhed, f.eks. hvis man glemmer sin laptop i taxaen eller lufthavnen ved et uheld.

Hvad kan man så gøre?

Overordnet set er der følgende indsatsområder:

- Uddan og træn jeres medarbejdere / Awareness
  - IT sikkerhedspolitik → Digital Fighters ApS
  - Shadow IT
  - CEO Fraud
  - Fysiske faktorer / Human errors
  - Insider Threat
- Beskyt dine virksomhedsdata
  - Domæne og DNS sikkerhed
  - Cloud sikkerhed, antispam, logins, MFA
  - Netværkssikkerhed, firewall, switche, wifi
  - Lokal sikkerhed, logins, pc, server, antivirus, antiransomware, antiPhishing, threat control, BitLocker.
- Opdater ALT
  - Herunder software, hardware, computere, smartdevices, netværksudstyr osv.
- Backup
  - Backup er det første du bør få styr på og forhåbentligt din sidste redning!

- Making IT work!

Opdatering / Patchning

Hvorfor patchning?

- ✓ Over 80% af alle angreb sker pga. ikke opdateret software
- ✓ Zero-days: Adobe og Java (ikke kaffen) er nok de meste kendte, og dem med flest ”huller”
- ✓ Sikkerhed – luk huller der måtte være i software!
- ✓ Oppetid – patchede systemer har typisk en højere oppetid, idet patchninger typisk også fixer fejl i softwaren.
- ✓ Efterleve standard – Revisionskrav? Kundekrav?
- ✓ Funktionsopdateringer – patches giver også jævnligt ny og/eller bedre funktionalitet i selve softwaren.

Hvad skal patches

- ✓ PC’er, servere, printere, mobile devices, netværksudstyr, IoT devices osv.

Hvad gør jeg for at imødekomme dette?

- ✓ Kontinuerlig automatiseret og monitoreret opdatering
- ✓ Windows Update dækker kun MS egen software – hvad med Adobe, Spotify eller de 300 andre stykker software du benytter
- ✓ Implementer et system, hvor du kontinuerligt kan holde øje med status – og gribe ind manuelt hvis det ikke fungerer.

- Making IT work!

Hvad kan man så gøre?

Overordnet set er der følgende indsatsområder:

- Uddan og træn jeres medarbejdere / Awareness
  - IT sikkerhedspolitik → Digital Fighters ApS
  - Shadow IT
  - CEO Fraud
  - Fysiske faktorer / Human errors
  - Insider Threat
- Beskyt dine virksomhedsdata
  - Domæne og DNS sikkerhed
  - Cloud sikkerhed, antispam, logins, MFA
  - Netværkssikkerhed, firewall, switche, wifi
  - Lokal sikkerhed, logins, pc, server, antivirus, antiransomware, antiPhishing, threat control, BitLocker.
- Opdater ALT
  - Herunder software, hardware, computere, smartdevices, netværksudstyr osv.
- Backup
  - Backup er det første du bør få styr på og forhåbentligt din sidste redning!

- Making IT work!

Backup

Backup, backup, backup – I må snart være trætte af at høre på det? …

Backup er din ABSOLUT sidste udvej, når alt andet fejler, så er der kun backuppen tilbage og derfor er det vigtigt at denne er af en ordentlig kvalitet.

Hvor ser vi fejl ved backup:

- Backup systemer der reelt kun laver en filkopi på et andet medie
- Backup systemer der ikke laver versioneret backup
- Backup systemer der ikke krypterer data at transport og at rest
- Backup systemer der er så dårlige/langsomme, at det er umuligt at lave en gendannelse.
- Backup der ikke fysisk er adskilt fra resten af netværket.

- Human error; ingen der kontrollere om hvorvidt en backup er kørt med succes eller fejlet.
- Human error; ingen der kontrollerer om en backup reelt kan gendannes.
- Human error; folk der tror at OneDrive, Dropbox, Google Drive osv. er backup.

Backup

Hvad er en god backup:

- ✓ Anerkendt løsning/software (Veeam, Acronis, Veritas, etc)
- ✓ 3-2-1 – 3 kopier af data på 2 forskellige medier og 1 offsite
- ✓ Offsite → Cloud
- ✓ Versioneret
- ✓ Krypteret
- ✓ Intelligent/Next-Gen backup → Tjek for nye virus/malware i selve backuppen, således at man ikke gen-inficeres over og over igen
- ✓ Monitorering og kontrol

Accept af at det koster noget og at det i mange cases bør være en cloud løsning.

- Making IT work!

nyit.dk

- Making IT work

Cyberforsikring

Topdanmark
Forsikring • Pension

Michael Hansen

- **Ansat i Topdanmark Forsikring 1/6-2002**

- **Solid erfaring med professionel rådgivning indenfor erhvervsforsikringer, Risk-management og pension til mellemstore og større erhvervs- og industrivirksomheder.**

- **Udover at være eksamineret assurandør med speciale i erhvervsforsikringer har jeg udbygget min kompetencer ved supplerende uddannelse på forsikringsakademiet.**

Indhold

- Hvad er cyber kriminalitet?
- Hvad dækker en cyber forsikring?
- Hvilke krav stilles der for forsikringsdækning?
- Cyber sikkerhedstjek
- Indvendinger imod cyberforsikring
- Skadeseksempler

• Hvad er cyber kriminalitet

Virus- og hackerangreb er en trussel, som erhvervsdrivende skal tage alvorligt. De kriminelle bliver hele tiden dygtigere og mere opfindsomme. I Danmark sker der et hackerangreb hver 20 sek.

Det er efterhånden hverdag for et stigende antal virksomheder at blive ramt af enten DDoS-angreb, hvor dit system overbelastes af hackere og derved lægges ned, eller af ransomware, hvor kriminelle låser dine data og kræver mindre beløb for at åbne op igen

Vidste du, at det tager en hacker syv minutter at bryde dit password på 8 cifre? 39 minutter, hvis du tilføjer et symbol.

Center for Cybersikkerhed i Forsvarets Efterretningstjeneste har konstateret, at cyberangreb udgør en stor trussel mod danske virksomheder. Nyeste undersøgelser viser, at 69% af danske virksomheder har været udsat for cyberkriminalitet.

De store virksomheder fortsætter med at øge deres investering i cybersikkerhed, dermed bliver de små- og mellemstore virksomheder et lettere mål og langt mere attraktive for cyberkriminelle.

Hvad dækker en Cyberforsikring

Forsikringen dækker rimelige, nødvendige og dokumenterede omkostninger til at genoprette sikredes IT-systemer og netværk og gendanne sikredes data, som følge af et angreb af ondsindet eller skadelig kode, herunder virus, samt hacker- eller Denial of Service-angreb.

Endvidere dækker forsikringen rimelige, nødvendige og dokumenterede omkostninger til at forhindre tredjemands misbrug af sikredes navn, logo, varemærke o.l., herunder til at lukke falske hjemmesider, der er oprettet for retsstridigt at udnytte eller skade sikrede eller dennes kunder.

IT beredskab 24/7 – 365 dage om året

77%

har været ramt af phishing angreb

58%

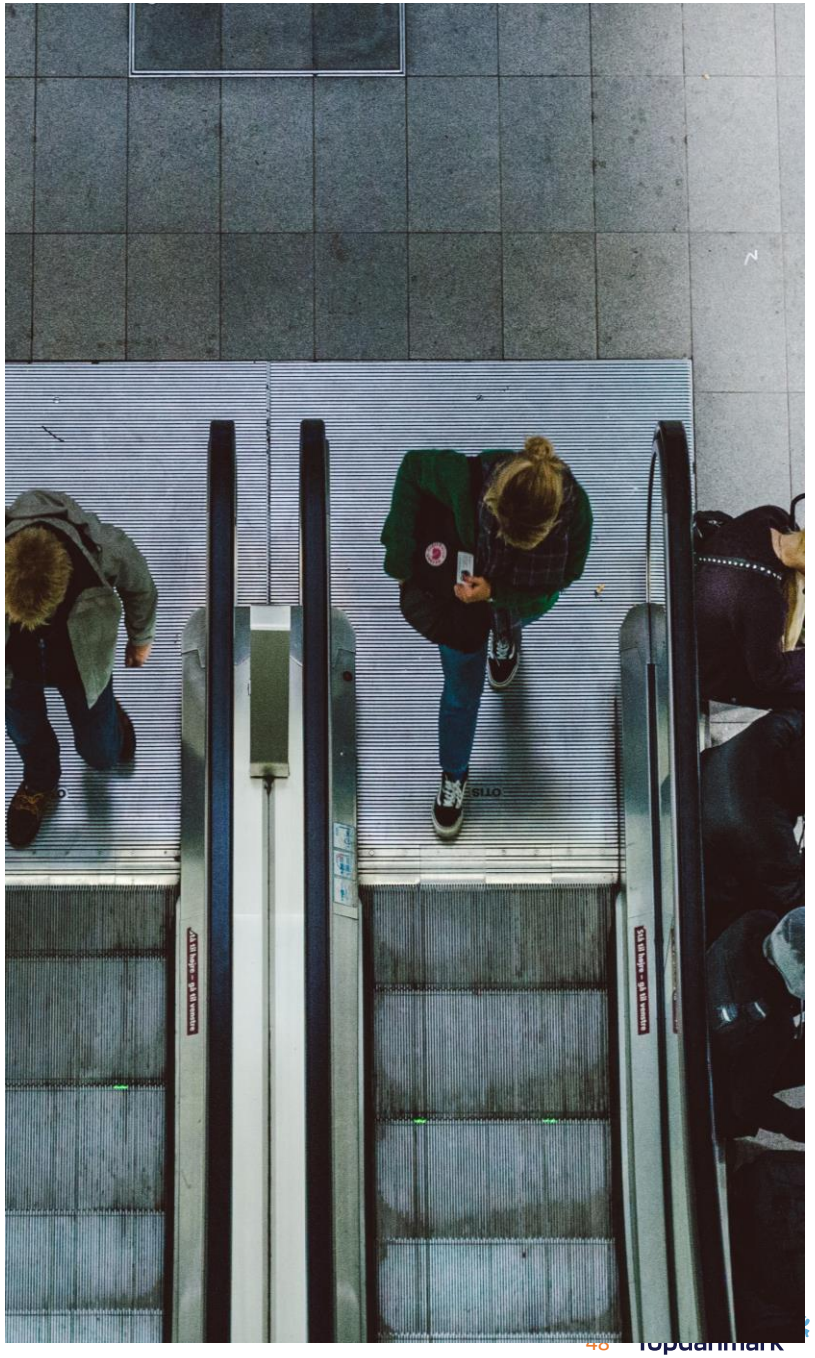
har været ramt af et ransomware angreb

52%

har været ramt af CEO Fraud

Cyber ansvar
- en del af grunddækningen

- Hackers misbrug af systemer til at gøre skade på andre
- Hackeres offentliggørelse af personfølsomme oplysninger
- Utilsigtet offentliggørelse eller videre sendelse af personfølsomme oplysninger ved brug af egne it-systemer
- Utilsigtet videre sendelse af virus mv. til tredjemand fra egne it-systemer
- Sagsomkostninger – også ved uberettigede krav
- Dækker hele verden



Cyber notifikationsdækning

- tilvalgsdækning

- Hvis virksomheden udsættes for en GDPR-skade er det virksomhedens ansvar, at redegøre for hændelsen og undersøge hvorfor den er sket, samt hvad der skal iværksættes for at standse skaden og underrette berørte
- Topdanmarks eksperter er klar til at hjælpe hele døgnet ved en skade
- Dækningen dækker omkostninger til notifikation til de personer/kunder som er berørte af datalækket
- Virksomheden har pligt til, at underrette Datatilsynet – det klarer Topdanmark som en del af dækningen

General Data Protection Regulation

Cyber driftstab

- tilvalgsdækning

Følgevirkningerne af et cyberangreb er ofte mere alvorlige end selve angrebet

Driftstab er den dækning, hvor vi udbetaler de største erstatninger

Topdanmark dækker op til tre måneder efter en skade – med en dags karenstid

Driftstab opgøres på samme måde, som ved en almindelig ”brandforsikring”

64%

af virksomhederne har været udsat for cybercrime de seneste 12 måneder

37%

af de ramte virksomheder mistede ikke blot penge som følge af cyberhændelserne, deres brand tog skade, de mistede kunder, og/eller kritiske systemer var utilgængelige

Ny dækning: ”Genoprettelse af renommé”

Ny ”PR-dækning” til genopretning af renommé efter en dækningsberettiget skade på basisdækningen

Dækker rimelige, nødvendige og dokumenterede omkostninger til brug af PR-bureau

Fast dækningssum på 250.000 kr. pr. år

En del af basisdækningen på samme måde som Cyberansvarsdækningen og dermed ikke en tilvalgsdækning

Sikkerhedsforholdsregler

Sikkerhedsforholdsreglerne gælder for cyberforsikring (pkt. 2), cyberdriftstab (pkt. 3), cyberansvar (pkt. 4) og notifikation (pkt. 5).

Som sikkerhedsforholdsregler gælder i henhold til forsikringsaftalelovens § 51 følgende:

Sikrede har til enhver tid pligt til at sikre:

a. At adgang til virksomhedens netværk og computere, bl.a. programmer og data, er sikret ved enten *multifaktor-identifikation**, ved kontrol af biometriske data (fingeraftryk mv.) eller ved password, der udskiftes minimum hver 6. måned. Alternativt kan der anvendes et stærkt password som er på minimum 12 karakterer og som anvender bogstaver, tal samt specialtegn.
b. At der anvendes firewall i virksomhedens netværk
c. At der på virksomhedens computere anvendes et opdateret antivirusprogram, herunder at virus-definitionsfilerne er opdaterede.
d. At indgående mails kontrolleres af et aktivt spamfilter
e. At der tages en indlæsbar backup mindst hver 5. arbejdsdag.
   Hvis backuppen opbevares online, skal den være placeret på et separat netværk, som ikke har adgang til virksomhedens driftsnetværk.
   Hvis backuppen opbevares offline, skal denne opbevares i et aflåst databrandskab eller aflåst i en anden *brandsektion** end der, hvor de pågældende data bliver brugt.
f. At mobiltelefoner og tavlecomputere (tablets), hvorfra der er adgang til sikredes IT-systemer, er sikret ved:
   1. At adgangen til den mobile enhed er beskyttet ved kontrol af biometriske data (fingeraftryk mv.) og/eller PIN-kode/et password
   2. At sikkerhedsopdateringer bliver installeret senest 1 måned efter frigivelse af disse
g. At adgangen til IT-udstyr, -systemer, -programmer og -data er sikret fysisk
h. At der er udarbejdet instrukser for installation og anvendelse af programmer, herunder forbud og sanktioner imod brug af piratprogrammer og imod anvendelse af uautoriserede tilslutbare enheder, herunder USB-drev og USB–nøgler, der kan tilsluttes en computer
i. At tilslutning til virksomhedens netværk udefra, fra f.eks. bærbare computere og mobiltelefoner, sker via en *sikker forbindelse**
j. At der foreligger en politik i forhold til tabte computere, mobiltelefoner, tablets mv., herunder at der sker politianmeldelse, såfremt der foreligger en mistanke om et kriminelt forhold, fx ved tyveri, røveri mv.

Er en eller flere af ovennævnte sikkerhedsforholdsregler overtrådt eller tilsidesat, gælder Topdanmarks forpligtelse for tab og omkostninger, som er omfattet af forsikringen, kun i det omfang det anses for godtgjort, at tabets indtræden eller omfang ikke skyldes sådan overtrædelse eller tilsidesættelse.

KAN DU SVARE JA TIL ALLE 12 SPØRGSMÅL?

Cyber sikkerhedstjek

Backup

- ✓ Tager vi backup hver dag?
- ✓ Kan vi gå en dag, en uge og en måned tilbage, hvis vores backup skal indlæses?
- ✓ Er vores backup beskyttet, så der KUN er adgang til den, når den er i brug?

Undgå altid, at der er adgang til NAS-bokse i netværket, hvis de anvendes til backup.

Beskyttelse af dit netværk

- ✓ Anvender vi en firewall, som beskytter os mod uautoriseret adgang?
- ✓ Anvender vi opdateret antivirus-beskyttelse på alle vores pc'er og servere?
- ✓ Har vi et opdateret spamfilter, som filtrerer uønskede mails fra?

Din anvendelse af it

- ✓ Anvender vi alle stærke password?

Dvs. min. 8 karakterer, store og små bogstaver, specialtegn og tal, som ikke er i rækkefølge.

- ✓ Kommunikerer vi altid kritiske ændringer som bank- og betalingsoplysninger ud til vores kunder på anden vis end at sende en e-mail?

... og ved vores kunder det?

- ✓ Når vi sender følsomme mails med fx PDF-fakturaer, opretter vi da altid en ny mail i stedet for at besvare en eksisterende korrespondance?
- ✓ Hvis vi modtager en mail, som vi er tvivl om, er ægte, sletter vi den så altid?!

Hvis vi er i tvivl, er vi ikke i tvivl.

Når du arbejder udefra

- ✓ Når vi logger på vores system udefra, er alle vores forbindelser så sikret udover blot brugernavn og password?

Envista anbefaler kraftigt , at der altid anvendes VPN eller tilsvarende sikkerhed.

Brug af eksterne systemer

- ✓ Anvender vi altid tofaktor-godkendelse, hvor det kan lade sig gøre?

Facebook, Gmail, MS 365, Google Adwords osv.

Typiske indvendinger imod cyberforsikringen

- *”Mine data er lagt i skyen (cloud løsning) – jeg har derfor ikke brug for en cyberforsikring”*

Stort set alle cloudvirksomheder benytter salgs og leveringsbetingelser, hvor de fraskriver sig alt ansvar. Med andre ord, kan man ikke rejse et krav mod cloudvirksomheden, hvis uheldet skulle være ude og man ender derfor selv med udgiften. Med en cyberforsikring vil man kunne få erstatning.

- *”Jeg kan sagtens arbejde, selvom mit IT skulle blive ramt. Vh Tømrermester Larsen”*

Det er ikke kun store virksomheder, som skal være på vagt. Håndværkere med få ansatte kan også blive ramt. At man stadig kan sende regninger ud til sine kunder samt vide, hvor man skal køre bilen hen for at arbejde må stadig være at foretrække. En cyberforsikring vil kunne hjælpe med dette.

- Jeg er bekymret for at få hijacket alt min data, og jeg er bekymret for, at jeg har flere biler, der står stille fordi, vi ikke kan komme videre. Jeg har brug for at en form for sikkerhed og forsikring om, at nogen har min ryg, hvis det går galt, siger Jonas Hemicke fra tømrer/snedkerfirmaet Fryd.

Typiske indvendinger imod cyberforsikringen

- **”Hvad skal jeg med den, jeg har et antivirusprogram?”**

Med et godt antivirusprogram er du beskyttet mod langt de fleste typer af angreb. Men selv det bedste antivirusprogram vil aldrig sikre dig 100 %, da hackerne hele tiden finder nye måder at angribe på.

- **”Jeg køber bare en ny computer, hvis jeg bliver ramt”**

Når hackerne først er inde i dine systemer, kommer de ikke lige ud igen. Hvis du er heldig, at dine filer kan overføres til en ny computer, kan det derfor gå galt igen. Vi ser ofte, at hackerne vender tilbage få uger efter.

56 % af de danske virksomheder var udsat for én eller flere sikkerhedshændelser i 2020.

Kilde: Pwc, Cybercrime Survey, 2021.

35.300 kr.

var den gennemsnitlige udbetaling pr. hackerangreb, der blev anmeldt til Topdanmark i 2019.

Kilde: Topdanmark, 2019.

Skadeeksempler

El-installatørs filer krypteret

En el-installatør, der ikke kunne få adgang til sit økonomisystem, opdagede, at alle filer på drevet var blevet krypteret. Han blev kontaktet af hackere, der krævede en løsesum for at låse filerne op. Angrebet mistænkes for at være startet ved et forkert klik på et link.

Ved ekstern IT-rådgivning lykkedes det at genskabe al data, men regningen løb alligevel op i 55.400 kr.

Revisionsfirma udsat for ransomware

Et hackerangreb på et revisionsfirma medførte, at alle computere blev låst. Flere revisorer kunne i flere dage derfor ikke indlevere regnskaber til tiden.

Skadeudgiften for driftstabet løb op i 122.000 kr.

Tøjbutiks IT-system låst af hackere

En tøjbutik blev udsat for et hackerangreb, hvor en såkaldt cryptolock-virus blev installeret i virksomhedens IT-system. Det betød, at alle butikkens IT-systemer var låst og ikke kunne tilgås.

Selvom det ved hjælp fra ekstern IT-support lykkedes at rense og genetablere tøjbutikkens IT-systemer, løb de samlede omkostninger op i mere end 95.000 kr.

Isenkræmmers webshop ramt af malware

En isenkræmmer opdagede, at hans hjemmeside var blevet ramt af malware, som gjorde, at et hacket betalingsvindue åbnede op i stedet for kundens eget.

Det lykkedes heldigvis ikke at få nogen kunder til at gennemføre betalinger i det nye betalingsvindue – men skadeudgiften for fjernelse af malware samt driftstab nåede at runde 82.000 kr.

Eksempel på en skade

- et advokatfirma blev hacket

- Forsikringstager har oplyst, at skaden skete, da en medarbejder klikkede på et link i en tilsendt mail. Dette bevirkede, at data på forsikringstagers SQL server og Exchangeserver, samt syv arbejdsstationer ud af i alt 35-40 stk. blev krypteret.
- Omfattet af skaden var bl.a. forsikringstagers advokatsystem. Efterfølgende viste det sig, at alle computerne var blevet inficeret med ransomware.
- Total skadesudgift = 290.000 kr.
- Det kostede 100.000 kr. at rydde op og driftstab beløb sig til 190.000 kr. for fem nede dage.

900 hoteller og kroer ramt på deres booking system

B.T.

JENS ANTON HAVSKOV HANSEN

900 hoteller og kroer i Danmark og det øvrige Norden samt Irland er nu på sjette døgn ramt af et ondsindet hackerangreb, som har sat booking- og betalingssystemet Picasso skakmat og har blokeret adgangen til alle data.

»Det er et mareridt. Vi famler jo totalt i blinde. Vi aner reelt ikke, om der for eksempel på lørdag er booket et selskab på 40-50 personer, som skal have måske seks retter mad. Og i givet fald aner vi ikke, hvad de skal have at spise. Eller om de har bestilt overnatning,« siger Finn Steffensen, som driver Nymindegab Kro med gourmetrestaurant og 44 værelser.

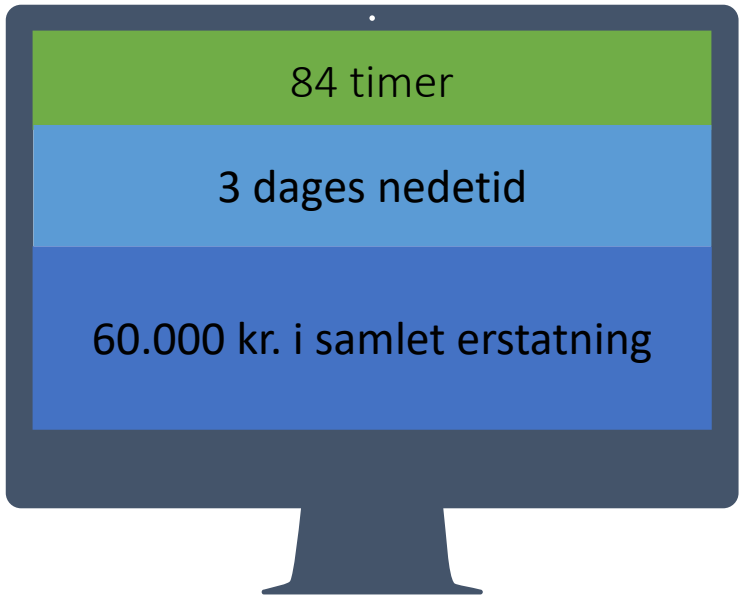
»Jeg har simpelthen så ondt i maven over det her. Det er en katastrofe,« siger han.

Han er formand for foreningen Small Danish Hotels, hvoraf 25 af dem med tilsammen 1.000 værelser er blandt de hoteller og kroer, der er ramt af hackerangrebet.

Skadeseksempler

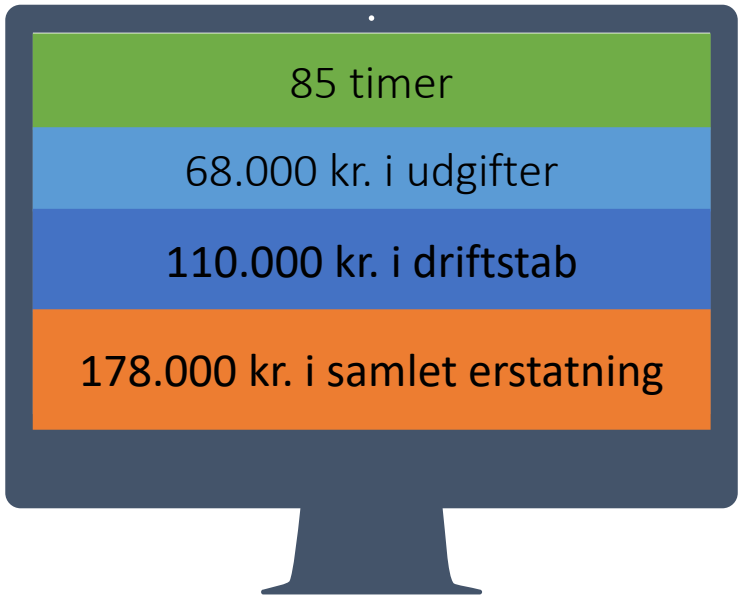
Nyt link i betalingsvindue

En isenkramforretning med webshop oplever, at deres kunder har problemer med at gennemføre en ordre. Hackere har fået adgang til virksomhedens systemer og har indsat et nyt link til betalingsvinduet, så betalingen ikke går til virksomheden.



Ransomware-angreb

En kunde der producerer maskiner til fiskeindustrien, blev ramt af ransomware-angreb, hvor alt deres data blev taget som ”gidsel” af hackere. Forsikringen dækkede disse udgifter.



Algoritme

En virksomhed der sælger tøj engros, blev udsat for cyberangreb. Via en algoritme fik hackere adgang til kundens systemer. Angrebet blev stoppet og kundens system renset. Forsikringen dækkede udgifterne.

Tak for jeres tid

- **Kontakt**
- Michael Hansen
Tlf. 29 44 67 61
mca@topdanmark.dk

Topdanmark