Det digitale trusselsbillede.

– Hvor er din virksomhed mest sårbar?

Håndbog til bedre IT-sikkerhed

Sådan navigerer du sikkert, når cybertrusler banker på i din virksomhed.

Mentor it
- med dig i fremtiden

Top 5: De største trusler

Phishing (79 %)

Finansiel svindel (CEO Fraud) (42 %)

Utilsigtet deling af følsom information, herunder personoplysninger (38 %)

Uautoriseret adgang til/brug af information, systemer eller netværk (34 %)

Hændelser forsaget af leverandørfejl (31 %)

Kilde: PwCs Cybercrime Survey 2020

Cyberkriminelle er eksperter i at udnytte svagheder i virksomheders økosystem og lokke medarbejdere til at begå fejl i en travl hverdag. Med øget opmærksomhed kan din virksomhed reducere risikoen for kompromittering og de økonomiske konsekvenser, der kan følge.

Den digitale udfordring

Erhvervslivet har de senere år været på en digital rejse, som kun tager mere og mere fart. Men med digitalisering følger ikke kun muligheder, - også trusler.

Cybersikkerhed er derfor blevet et vigtigt tema, som nyere tal fra flere undersøgelser kun bekræfter. Antallet af cyberangreb er stigende.

Dette er en vejledning til, hvordan I i direktionen og ledelsen navigerer bedst i det aktuelle trusselsbillede. Vi har samlet nogle konkrete bud på, hvordan I kan løse udfordringerne og løfte virksomhedens sikkerhedsniveau.

God fornøjelse.

Det digitale trusselsbillede

Vores måde at arbejde på digitaliseres dag for dag. Mulighederne inden for IoT, kommunikation, industri og praktik ekspanderer – og det samme gør risikoen for cyberangreb. Vores sårbarheder bliver flere.

Det er ikke et spørgsmål, om det sker, men hvornår det sker

Antallet af sikkerhedshændelser øges år for år. Truslen er ikke kun rettet store virksomheder, men alle.

Hvem er vi oppe i mod?

De fleste cyberangreb udføres af organiserede kriminelle, som udnytter de svagheder, der er i virksomhedens digitale netværk. De bruger så disse til at stjæle information eller fuldføre ransomware-angreb med økonomisk vinding som resultat.

Det er organisk og ændres konstant

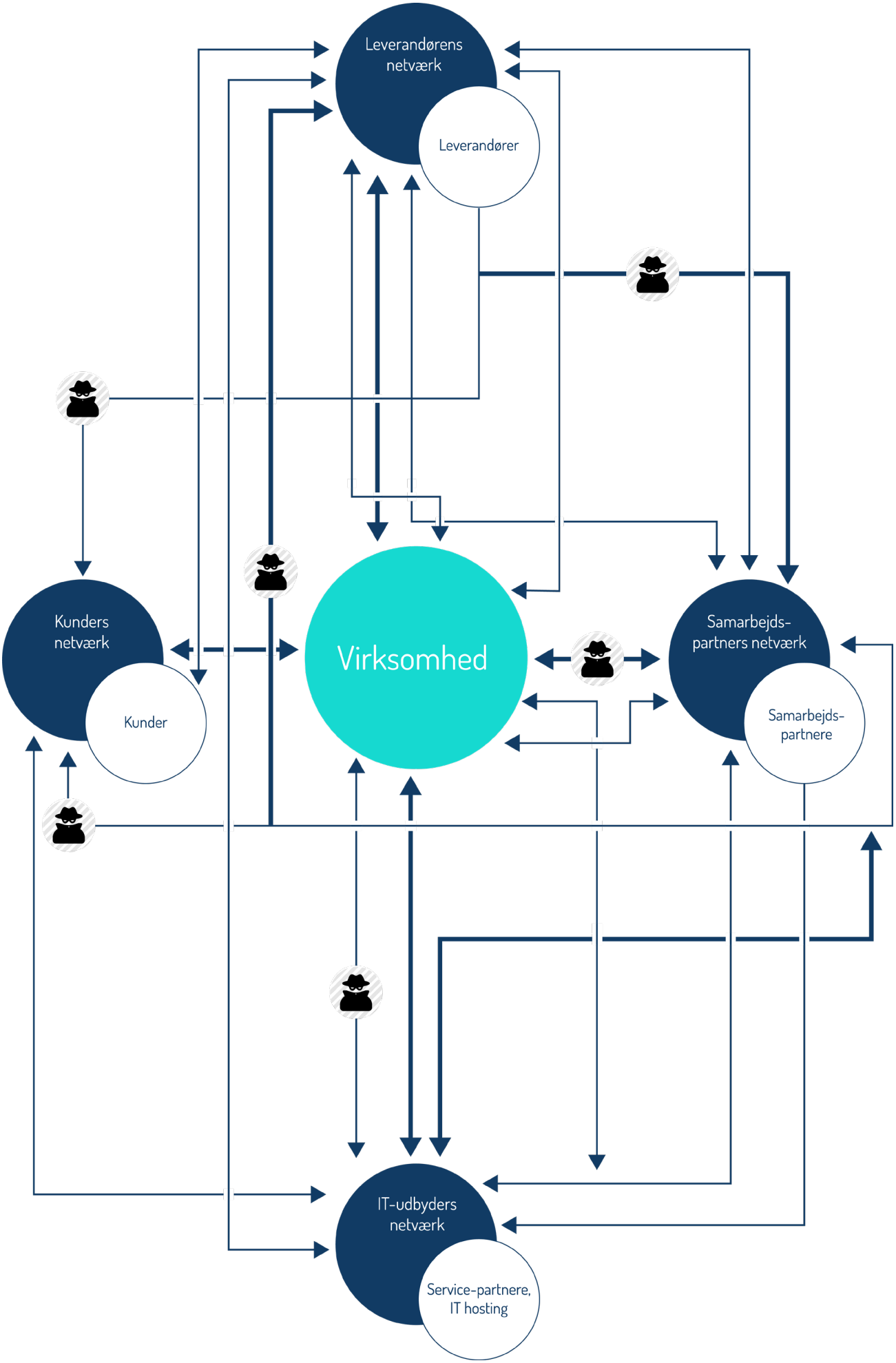
Vi oplever lige nu det højeste antal af sikkerhedshændelser i fire år. 58 % angiver, at de har været udsat for én eller flere sikkerhedshændelser inden for de seneste 12 måneder.

Antallet af phishingangreb har aldrig været højere. 79 % af dem, der har været udsat for en sikkerhedshændelse siger, at de var udsat for phishingangreb.

Èt ud af tre phishingangreb har været relateret til covid-19 pandemien. 35 % fortæller, at af phishingangrebene i nogen grad eller høj grad var relateret til covid-19 pandemien.

Økosystemets svagheder

Din virksomhed er dagligt i dialog med leverandører, samarbejdspartnere, kunder og øvrige servicepartnere. Det giver mange snitflader og skaber svagheder i det digitale netværk, som organiserede kriminelle kan udnytte.
Det kræver kun ét svagt led i dit økosystem.


Leverandørens netværk
Leverandører
Kunders netværk
Kunder
Virksomhed
Samarbejds-partners netværk
Samarbejds-partnere
IT-udbyders netværk
Service-partnere, IT hosting

Typiske hændelser

Selvom nutidens cyberkriminelle er forholdsvis organiserede og hele tiden bliver mere professionelle, er deres motiv ofte kortsigtet. Det handler om hurtig økonomisk gevinst eller indsamling af information, som kan give økonomisk gevinst på lidt længere sigt men stadig inden for en nær fremtid.

Phishing

I 2020 oplevede danske virksomheder rekordmange phishingangreb. Det er den mest hyppige type cyberangreb. Hele 79 % af de virksomheder, som har været udsat for cyberangreb, har været udsat for phishing.

Phishingangreb er et forsøg på at udnytte svage led i dit økosystem. Eksempelvis en travl medarbejder. Cyberkriminelle udgiver sig for at være en troværdig virksomhed eller organisation. Det kan være en offentlig myndighed eller din bank. Formålet er at få modtagerne til at overføre penge eller information. Formålet kan også være at lokke modtagerne til at klikke på et link, der låser virksomheden filer – hvorefter der kan kræves løsesum.

Klassiske eksempler på phishingmails kan indeholde:

- Du skal overføre penge til en specifik konto.
- Du bliver bedt om at nulstille dit password.
- Du skal opdatere personlige information i et regneark eller ved at klikke på et link.

At forebygge phishing handler om opmærksomhed. For de cyberkriminelle bliver bedre og bedre til phishing, der ser troværdig ud. Det gælder både at efterligne officielle logoer og bedre formuleringer.

Sådan undgår du og dine medarbejdere at blive lokket af phishing

1. Er afsenders mailadresse valid?

Hvis ikke adressen kan ses, kan du klikke på afsenders navn, og adressen vil komme frem. Her kan du blandt andet tjekke, om domænet (teksten efter @) er troværdig og i overensstemmelse med virkeligheden. @skat1234.dk er for eksempel ikke dén Skat, som typisk sender din forskudsopgørelse.

2. Er budskab, sprog og stavning troværdig?

Måden, hvorpå en e-mail er formuleret, kan ofte afsløre, om den er sand eller falsk. Sprogfejl og stavefejl var hyppigt engang, når man modtog phishingmails. Det er ikke så slemt længere, men småfejl optræder fortsat, og det kræver din opmærksomhed at spotte dem.

3. Er der links eller vedhæftede filer, du opfordres til at klikke på?

Typisk vil du blive bedt om at klikke på et link, åbne en fil eller sende noget bestemt retur til afsender. Alle tre opfordringer kan være et tegn på phishing.

4. Er mailsignaturen oprigtig?

Phishingmails har sjældent en mailsignatur, der er i overensstemmelse med, hvad du normalt oplever. Se efter, om den er mangelfuld og ulig normalen. Vær særligt ekstra opmærksom, hvis der blot er indsat: Sendt fra min iPhone.

Vil du mere om phishing?
Download medarbejderhåndbog om phishing

CEO Fraud

CEO-Fraud, der også kendes som direktørsvindel, er falske e-mails eller SMS'er. De bliver sendt, så det ligner en besked fra en direktør eller leder til øvrige medarbejdere.

Oftest sendes disse e-mails fra en falsk og fremmed mailkonto og blot med direktørens navn. I nogle tilfælde kan cyberkriminelle dog have fået adgang til den rigtig mailkonto, og dermed kunne sende direkte derfra.

De falske e-mails har til formål at få medarbejderen til at betale falske fakturaer eller lave andre for former for betalinger. Oftest med en tone af, at det haster.

Sådan undgår du og dine medarbejdere at blive narret af CEO-fraud

1. Tjek afsenderens e-mailadresse

Første trin er altid at tjekke e-mailadressen, som besked kommer fra. Her kan du som regel sortere de fleste falske henvendelser fra.

2. Dobbeltjek med din chef

Kontakt altid din chef for at dobbelttjekke, hvis du bliver bedt om at lave betalinger eller overførsler over e-mail.

3. Vær særligt opmærksom i ferier

Mange cyberkriminelle bruger særligt ferieperioder til CEO-fraud. I disse perioder er der ofte færre medarbejdere og ledere på arbejde i virksomheden – og dermed færre til at dobbelttjekke forespørgslen.

Ransomware

Ransomware er kort fortalt et stykke ondsindet kode, som kan plantes på virksomhedens computere eller netværk. Koden kan kryptere virksomhedens data, så de cyberkriminelle efterfølgende kan afpresse virksomheden.

Der er oftest tale om en løsesum, der skal betales i Bitcoins for at få adgang til de krypterede data igen.

Vejen til beskyttelse mod ransomware går gennem grundlæggende IT-sikkerhed.

Sådan forebygger du at blive ramt at ransomware

1. Vedhæftede filer

Vær skeptisk, hvis du modtager vedhæftede filer fra brugere, du ikke kender. Undlad at åbne eller installere filer. Oftest kommer filer fra cyberkriminelle i formaterne zip, rar eller src.

2. Skjulte links

Hold altid musen hen over et link, før du klikker på det. Så kan du se, hvor det peger hen. Et link kan sagtens skjules bag en tekst (eller et andet link). Hvis link og afsender ikke matcher, kan det være tegn på cyberkriminalitet. Åben derfor hellere din browser og skriv afsenderens webadresse manuelt.

3. Reelle afsendere

Offentlige instanser, organisationer og andre reelle afsendere er i dag meget opmærksomme på potentiel cyberkriminalitet, hvor de bruges som dække. Derfor vil en reel afsender som eksempelvis Skat.dk, PostNord eller din bank aldrig bede dig klikke på et link for at verificere oplysninger eller lave betalinger.

4. Basal IT-sikkerhed

Derudover er opdatering af systemer, applikationer, netværk mv. helt centralt i kampen mod ransomware. Brug tofaktor-godkendelse, sikker fjernadgang og kryptering, hvor det er muligt og giver mening i jeres virksomhed. Tag gerne en rådgiver med speciale i IT-sikkerhed med på råd.

Den menneskelige faktor: Medarbejderne

Menneskelige fejl er ofte grunden til, at hackere lykkes med deres ondsindede handlinger. De ved lige præcis, hvordan de kan lokke medarbejdere til at begå fejl, som kan kompromittere virksomheden.

Løbende træning og uddannelse af medarbejdere i IT-sikkerhed er derfor vigtigt. Som virksomhed bør man opbygge en kultur, hvor sikkerhed indgår og kan bidrage til at reducere virksomhedens sårbarhed. En rapport fra Erhvervsstyrelsen i 2020 viser, at netop virksomhedskulturen ofte er en barriere for SMV'er i forhold til IT-sikkerhed.

Sådan forebygger du menneskelige fejl

1. Oplysning og opmærksomhed

Opskriften er simpel, selvom den er kan være kompleks at implementere. Den handler om oplysning, uddannelse og opmærksomhed.

Hvis både ledelse og medarbejdere er opmærksomme på lurende cybertrusler for virksomheden, kan det gøre en forskel. Hvis medarbejderne eksempelvis kan identificere klassiske phishingmails eller lignende, falder risikoen for cyberangreb mærkbart.

2. Tofaktorgodkendelse

Som IT-bruger er man blandt virksomhedens største risici. Derfor er tofaktorgodkendelse et populært værktøj. Med et ekstra sikkerhedslag skærpes adgangen til din virksomheds data.

Tofaktorgodkendelse sikrer, at et login ikke kan gennemføres uden verificering – selvom medarbejderen har fået franarret sine loginoplysninger.

3. Backup

Bliver din virksomhed alligevel ramt af et cyberangreb, er automatisk backup af systemer, filer mv. jeres bedste værktøj til at komme tilbage på benene – tilbage til normal drift og med mindsket nedetid.

Hvordan ser jeres trusselsbillede ud?

Med en analyse eller gennemgang af jeres IT-sikkerhed, kan I få indblik i, hvordan jeres trusselbillede i virksomheden ser ud. Spørg din IT-leverandør om hjælp og find ud af, hvordan I bedst kommer i gang.

Ved Mentor IT har vi udviklet et Sikkerheds-barometer, som identificerer jeres styrker og svagheder og ved hjælp af en simpel pointscore, indikerer sikkerhedstrykket i jeres virksomhed.

Sikkerhedsbarometeret behandler seks sikkerhedsområder og definerer både sikkerhedsniveauet pr. område og samlet.

Konkret udmøntes barometers findings i en rapport, som I kan bruge til at optimere jeres sikkerhed. I kan samtidigt genbesøge barometeret på et senere tidspunkt og få lavet en ny analyse, der belyser udviklingen. På den måde kan I arbejde fokuseret og kontinuerligt med IT-sikkerhed.

Vil du gerne vide mere om vores Sikkerheds-barometer?

Kontakt os på +45 70 122 123.
Sammen gør vi din IT mere sikker.

Anbefalet minimum

79 point

ud af 138 point

..i tvivl?

Har du spørgsmål, eller er du det mindste i tvivl om, hvordan du og dine kollegaer bedst navigerer i det nuværende trusselsbillede? Så sig endelig til. Vi hjælper gerne med at skabe mere sikre og trygge arbejdsrammer.

God fornøjelse!

Mentor IT Esbjerg
Mentor IT Kolding
Mentor IT København
Mentor IT Aarhus

Telefon +45 70 122 123
E-mail info@mentor-it.dk

Mentor it
- med dig i fremtiden