wingmen

Sådan sikrer du din forretning mod cyberangreb

Alle virksomheder er truet - har du styr på din Endpoint Security?

Indhold:

Derfor er Endpoint Security det væsentligste sikkerhedsspørgsmål for din virksomhed lige nu

Cybersikkerhed er i bund og grund et våbenkapløb mellem hackere (og deres kriminelle bagmænd) og virksomhederne. Hackerne er desværre ofte et skridt foran, og derfor er det de IT-sikkerhedsansvarliges opgave konstant at sikre, at der ikke er nogle sprækker i virksomhedens netværk, hvor hackerne kan skaffe sig adgang. Har de først adgang, kan konsekvenserne ved cyberangrebet være uoverskuelige. I værste fald er din forretning færdig for altid.

Trusler og tendenser inden for cybersikkerhed er derfor i konstant bevægelse. Hos Wingmen har vi i disse år særlig fokus på Endpoint Security. Det vil sige sikkerheden på virksomhedens arbejdsstationer, mobile enheder og andre enheder, der er forbundet til jeres netværk, og som således er indgange til jeres datacenter og cloud-løsning.

Endpoint Security er centralt for virksomhedernes cybersikkerhed:

Vi er alle forbundet

Virksomheder, organisationer, myndigheder og privatpersoner har forskellige udfordringer i forhold til cybersikkerhed og opererer med forskellige grader af sikkerhed, systemer, adfærdsmønstre, mv. Idet vi alle er forbundet og udveksler data på kryds og tværs af platforme, datacentre og servere, er alle kontaktpunkter med din virksomhed derfor potentielle indgange (direkte og indirekte) for hackere.

Vi arbejder decentralt

Flere og flere arbejder hjemme og decentralt. De nye arbejdsformer gør arbejdsstationerne mere udsatte for angreb, da de ofte er koblet på usikre netværk, og da medarbejdernes brug af de mobile arbejdsstationer er anderledes, end når de sidder bag de stationære maskiner på kontoret.

IoT giver nye udfordringer

IoT (Internet of Things) har vist sig at være en ny og større trussel, end hvad man havde forestillet sig. I de fleste kontorer og bygninger er alt fra dørlåse til lysstyring, køleskabe og mødelokaler koblet på netværket. IoT-objekterne er ofte både dårligt sikret og svære at tilgå for virksomhedens teknikere - fx kan du ikke installere antivirus software på et køleskab. Men hackerne finder nemt vej og ved, hvordan de kan plante et stykke kode, som kan sprede sig til resten af netværket.

Den gode nyhed er imidlertid, at der er en række tekniske tiltag, du kan foretage for at mindske risikoen for og effekten af et angreb. Samtidig bør du udarbejde en contingency plan (beredskabsplan), så du og resten af organisationen ved, hvordan I håndterer et angreb, hvis uheldet er ude.

Cisco AMPs tre trin til bedre cybersikkerhed:

Prevent

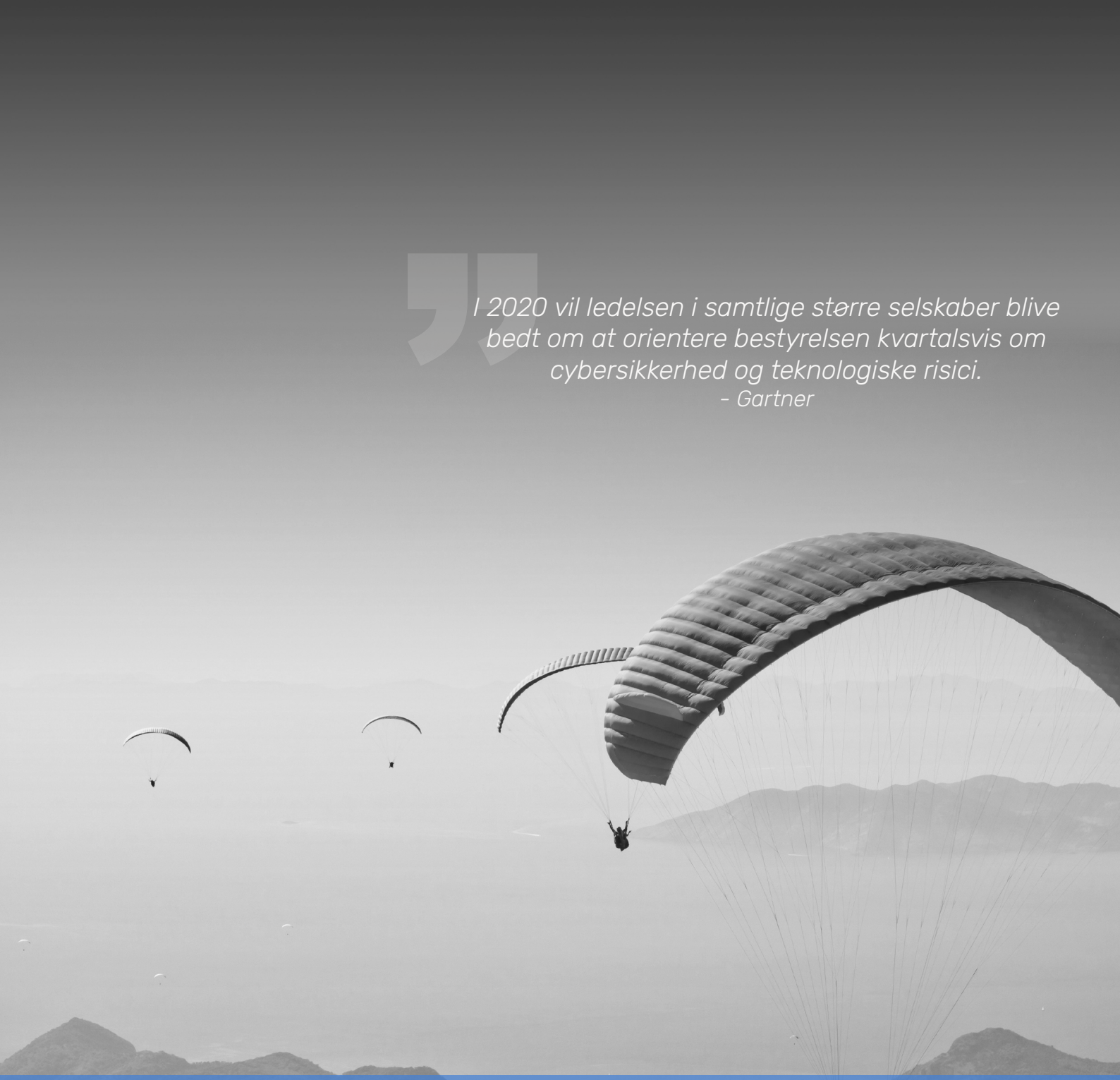
Blokér malware på alle endpoints og arbejd med segmentering i dit netværk, så ikke alle endepunkter har adgang til alt. Sørg for, at du er opdateret på alle kendte aktuelle trusler ved at koble dig op på et internationalt sikkerhedsnetværk som Cisco Talos <Link: https://talosintelligence.com/>, som registrerer malware og alle vira.

Detect

Gennemsøg konstant dit netværk for skjulte trusler og malware i dvale. Hold øje med, hvad en kode gør, som er unormalt, og ikke kun hvilken kode der er tale om. Ikke alt malware bliver identificeret ved endpoints.

Respond

Er uheldet ude, skal du hurtigt indkapsle malwaren, isolere de inficerede endpoints og få overblik over, om malwaren har spredt sig. Aktivér din contingency plan.



I 2020 vil ledelsen i samtlige større selskaber blive bedt om at orientere bestyrelsen kvartalsvis om cybersikkerhed og teknologiske risici.
- Gartner

Cybersikkerhed handler om din kerneforretning

Cybersikkerhed handler langt fra kun om teknik og er ikke blot noget, IT-afdelingen skal tage sig af. Det handler om muligheden for at drive, udvikle og tage vare på din kerneforretning, herunder måden din organisation arbejder på, og måden I er i kontakt med jeres kunder på. Så selvom de praktiske elementer i cybersikkerhed starter og slutter i IT-afdelingen, er der mange forretningskritiske beslutninger, du og resten af virksomhedens ledelse skal tage, inden det er for sent.

I takt med den omfattende digitalisering af samfundet og erhvervslivet er stort set alle områder, som har betydning for driften af din virksomhed - ja, for hele samfundet - eksponeret for cyberangreb, herunder:

- Netværk og IT-udstyr
- Produktionsmaskiner og bygninger
- Personfølsomme data (kunder og medarbejdere)
- Immaterielle rettigheder (IP) og patenter
- Kritisk infrastruktur

Samtidig betyder den skærpede lovgivning omkring datahåndtering, at cybersikkerhed ikke er et område, hvor den enkelte virksomhed suverænt selv kan lægge snittet. Er uheldet ude og personfølsomme data bliver eksponeret, skal I forberede jer på sagsanlæg og et retsligt efterspil med myndighederne i de berørte lande.

Hvis vi skal lidt ned på jorden igen og blive meget konkrete, så afhænger jeres oplevelse af et cyberangreb - og den økonomiske konsekvens angrebet har - af jeres virksomhed, kerneydelse og organisering. Derfor bør I i forbindelse med det kontinuerlige arbejde med jeres Endpoint Security og samlede IT-sikkerhed opstille scenarier for, hvad det i praksis betyder for jeres forretning og daglige drift, hvis jeres netværk bliver angrebet.

Et par eksempler fra virkelighedens verden:

Har I butikker landet over tilkoblet et centralt lager- og ordresystem, kan I måske ikke sælge noget, hvis kasseapparaterne ikke kan få forbindelse til serveren, eller hvis de slet ikke kører. Har I et fuldt digitaliseret lager, kan I ikke hente (og dermed sælge) så meget som en knappenål, da kun robotten ved på hvilken lagerhylde, den ligger. Er jeres produktion digitaliseret med IoT-udstyr (transportbånd, robotter, mv.), står produktionen stille.

Er I en webbaseret virksomhed, går kunderne til konkurrenten med et enkelt klik, når dit website er nede. Samtlige af jeres medarbejdere vil være ude af stand til at arbejde, uagtet om de sidder ved frontdesk, back-office eller i produktionen. Hvis I er et børsnoteret selskab, vil jeres børsværdi falde, fordi I hverken kan sælge eller producere - det kan påvirke muligheden for at tiltrække fremtidig investering… Og så har vi ikke engang nævnt skadevirkning som følge af tyveri af data, immaterielle rettigheder og forretningshemmeligheder.

Cyberangreb rammer alle typer af virksomheder

I modsætning til hvad mange tror, er cyberangreb ikke noget, der kun rammer store velkendte virksomheder og brands med svimlende omsætningstal og velpolstrede kapitalreserver, som hackerne kan dykke ned i. Mindre og mellemstore virksomheder er også udsatte. På mange områder er de ligefrem mere attraktive mål for hackere end de globale giganter.

De fleste cyberangreb handler om penge.

Derfor må hackerne vurdere balancen mellem, hvor let det er at få adgang til en virksomhed, og hvor stor en løsesum de kan få ud af virksomheden via ransomware. Typisk er store organisationer bedre sikret end mindre og mellemstore virksomheder, som i mange tilfælde har et meget traditionelt sikkerheds-setup baseret på standard antivirus-software og firewalls. Derfor bliver det pludselig attraktivt at foretage skalerede angreb på mange små virksomheder, hvor sandsynligheden for, at hackeren får sin løsesum hjem, er mange gange større end ved enkeltstående komplekse angreb på store virksomheder. Hurtig adgang til 500 x 100.000 kr. er mere værd end svær adgang til 50 mio. kr.

Vi hører sjældent om angreb på mindre virksomheder i medierne, og det er en medvirkende faktor til, at mange ikke føler sig udsatte. Men truslen er reel, og både afpresning via ransomware og informationstyveri er i eksplosiv vækst i disse år.

Det seneste halve år, hvor alle typer af virksomheder har opereret i skyggen af COVID-19, har i den grad sat fokus på, hvor stor risikoen reelt er i forhold til Endpoint Security. I en ny undersøgelse præsenteret i Security Magazine svarer 34 % af de IT-sikkerhedsansvarlige, at de frygter, at de ansatte har fået en for afslappet holdning til sikkerhed, på grund af deres fysiske omgivelser, når de arbejder hjemme. I samme undersøgelse fremgår det også, at der i denne særlige sårbare periode har været en markant stigning i antallet af angreb via samtlige angrebsvektorer i virksomheden.

Men den største og mest foruroligende overraskelse i undersøgelsen er nok, at halvdelen af de adspurgte IT-sikkerhedsansvarlige ikke havde en contingency plan (beredskabsplan) i tilfælde af et angreb!

Eksempler på alvorlige cyberangreb fra det seneste årti:

Stuxnet 2010	Iranske centrifuger til berigelse af uran blev fysisk beskadiget som følge af et cyberangreb med Stuxnet-malware.
Saudi Aramco 2012	Det saudiske olie- og gasselskab Saudi Aramco fik ødelagt store mængder af virksomhedens data under et cyberangreb.
The Sony Hack 2014	Det amerikanske filmselskabv Sony Pictures Entertainment fik ødelagt data og systemer samt lækket e-mails og kopier af kommende film.
Strømafbrydelsen i Ukraine 2015	En række elektricitetsværker i det vestlige Ukraine blev ramt af cyberangreb. Hackerne fik adgang til virksomhedernes kontrolsystemer og slukkede for strømmen i op til 6 timer.
DMC 2016	Det amerikanske politiske parti Demokraterne var målet for et hackerangreb og læk af informationer - herunder e-mails - kort inden præsidentvalget samme år.
WannaCry 2017	WannaCry-ransomware spredte sig automatisk til computere verden over i maj 2017. Filer på ofrenes computere blev krypteret, og originale filer blev slettet.
OPCW 2018	De hollandske myndigheder tog russiske efterretningsagenter på fersk gerning i færd med at tilegne sig adgang til Organization for Prohibition of Chemical Weapons (OPCW) netværk.
Demant 2019	Den danske høreapparatproducent Demant var målet for et ransomware-angreb. De økonomiske tab fra angrebet estimeres at være op til 650 mio. kr.
Georgia 2019	Den amerikanske delstat blev ramt af et stort antal cyber-angreb, som lukkede tre tv-stationer og over 2.000 websites ned.
ISS 2020	Den internationale servicevirksomhed ISS blev lagt ned af et cyberangreb. Derudover blev der bl.a. ekstraheret personfølsomme data på 65.000 medarbejdere. Under pressemødet blev ISS 3,5 milliarder mindre værd for investorerne.

Derfor skal du have en contingency plan

Ligesom med alle andre former for kriser, så er det jeres evne til at håndtere et cyberangreb, som afgør, hvad konsekvenserne af angrebet bliver for jeres virksomhed, og hvordan jeres kunder og interessenter efterfølgende dømmer jer. Her er jeres contingency plan det vigtigste værktøj.

Et typisk cyberangreb:

1. En medarbejder klikker på et link og får hentet malware ned.
2. Koden ligger i dvale i en periode.
3. Koden vågner - eller bliver aktiveret udefra - og får kontrol over medarbejderens pc.
4. Koden spreder sig til de dele af netværket, brugeren har adgang til.
5. Virksomhedens data bliver krypteret (ransomware) eller ekstraheret.

Din contingency plan skal sikre, at cyberangrebet kommer under kontrol, og at jeres virksomhed kommer tilbage til normal drift så hurtigt som muligt. Derfor skal planen klart og tydeligt angive rollefordelinger og ansvarsområder, ligesom den skal indeholde tekniske guidelines til, hvordan I indkapsler malware og genopretter jeres systemer.

Det er ikke så enkelt, som det lyder. For det første er to cyberangreb sjældent ens. For det andet har man tendens til at spekulere i enkeltstående fejl og nedbrud, og derfor bliver simultane fejl svære at håndtere - for hvad gør man, hvis begge redundante datasæt er inficeret med malware?

For det tredje er der risiko for, at contingency planen bliver mere teoretisk end egentlig operationel og i praksis ikke løser noget som helst. Derfor skal I først og fremmest fokusere på at have en basisplan, som klart og tydeligt angiver:

Kommunikation
Hvem skal have hvad at vide? Hvordan får I informeret alle medarbejdere, hvis jeres netværk er nede? Hvordan får I advaret medarbejderne om, at de ikke må åbne deres pc?

Primær beskyttelse
Hvad er livsnødvendigt for jeres virksomhed? Hvordan beskytter I det?

Hvem I ringer til
Har I en beredskabsaftale med eksterne konsulenter?

Som led i arbejdet med contingency planen skal I - i lighed med scenarierne for konsekvenserne for jeres daglige drift - opstille forskellige scenarier for, hvordan I genopretter jeres system i et worst-case-scenario, hvor I skal starte hele netværket op fra grunden som led i et regulært disaster recovery:
Hvilken maskine er den første I tænder? Hvordan sikrer I, at den maskine ikke er inficeret? Hvor lang tid tager det at indlæse en fuld backup på en server? Hvor lang tid tager det at indlæse backup på 1.000 servere på mange lokationer?

Hvordan er afhængighederne mellem forskellige maskiner, segmenter og dele af netværket? Kan I stå med et catch-22, hvor I ikke kan starte maskiner op, fordi de er gensidigt afhængige, men en af dem er inficeret? Hvordan er I i dialog, hvis jeres telefonsystem er på netværket… som er ude af drift? Og hvordan kommer I i det hele taget ind i bygningen, hvis jeres fysiske adgangssystem er inficeret?

Samtidig bør I have fokus på løbende medarbejdertræning i digital adfærd, ligesom I - selvom det er ressourcekrævende - løbende bør teste jeres beredskab.

Tak for at du læste Wingmens e-bog om cybersikkerhed.

Vi håber, at du har fået øget indblik i, hvorfor Endpoint Security er et centralt element i din cybersikkerhed, hvad cybersikkerhed betyder for din virksomhed og forretning, og hvorfor du bør have en contingency plan.

Vi kan også hjælpe dig med at styrke din Endpoint Security, bl.a. gennem nogle af de indsatser og fokusområder vi har omtalt her i e-bogen.

Vi er certificeret Cisco Guld-partner og eksperter i netværk, datacenter og sikkerhed. I forhold til jeres overordnede cybersikkerhed, herunder jeres Endpoint Security, kan vi stå for implementering af Cisco Umbrella, AMP og Duo i jeres datacenter og samlede netværk.

Kontakt os for et uforpligtende møde.

København
Tobaksvejen 23B, 1. sal th.
2860 Søborg

Århus
Lyshøjen 2, 1. Sal tv.
8520 Lystrup

Telefon: 70202110
info@wingmen.dk
CVR: 36440228

wingmen

CISCO
Partner