CHECKLISTE

Hvordan du beskytter din organisation mod ransomware

Forord

Cyberkriminalitet er blevet en meget profitabel forretning i de senere år. Faktisk spås cyberkriminalitet at koste verdenssamfundet et to-cifret trillion-beløb ved udgangen af 2025.
Vi stiller her skarpt på, hvordan du bedst kan beskytte din virksomhed mod et af de mest almindelige angrebstyper.

Ransomware dukkede først op i verdensbilledet i 80'erne, og er siden blevet et af de mest almindelige angrebstyper i verden. Et ransomware-angreb er i korte træk, når hackere tvinger sig adgang til følsomme data, og derefter krypterer det, så det ikke længere er tilgængeligt for ejeren. De sætter sig derved på dataen, og kræver en løsesum for at frigive eller levere dataen tilbage.
I de senere år er ransomware blevet mere og mere professionaliseret, og vi ser bl.a. et stigende antal hackere, der tilbyder at udføre ransomware-angreb som en service. Med kryptobetalinger og en hurtig søgning på dark web kan de fleste relativt let angribe en virksomhed, og antallet af hackerangreb er stødt stigende – 64% stigning i angreb på virksomheder fra 2021 til 2022.

Med AI-baserede værktøjer er det lettere end nogensinde for cyberkriminelle at finde frem til sårbarheder og nye ofre.
Det er ikke længere et spørgsmål om, hvorvidt en virksomhed rammes, men mere et spørgsmål om hvornår. Så hvordan kan I stå stærkt, når det sker?
Her har vi samlet ni gode råd til, hvordan din virksomhed kan opruste jeres beredskab mod en af tidens største trusler.

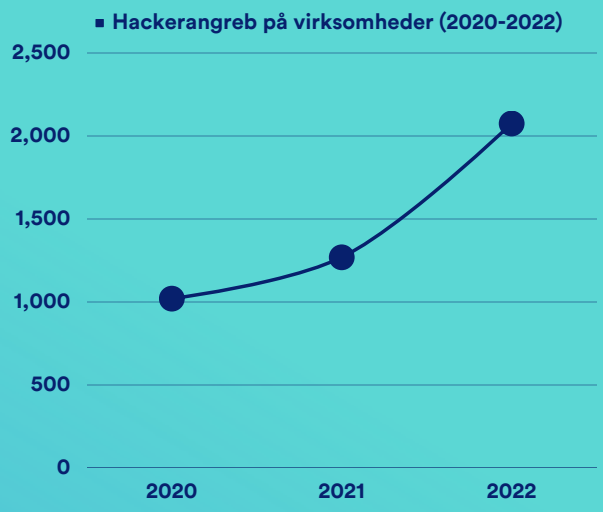
Hvordan ser ransomware ud?

Tre almindelige typer ransomware-angreb

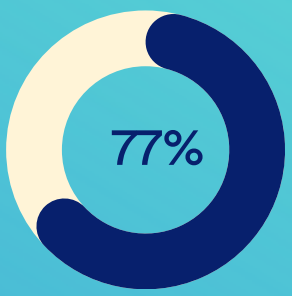
1 Eksisterende sårbarheder

En af de typer angreb, vi ofte ser, er udnyttelse af en virksomheds eksisterende sårbarheder. Det er bl.a. en af årsagerne til, at virksomheder holder kortene tæt til kroppen, når deres systemer angribes. I dag er det ofte sådan, at hackere bruger et system til at scanne for eksisterende huller i sikkerheden, f.eks. fejlagtige systemintegrationer eller fejlplacerede logininformationer. Så snart en sikkerhedsbrist opstår, dukker den op på hackernes radar indenfor blot 72 timer, og når først hackerne er trængt ind, går det stærkt – indenfor kun 2 timer kan de have krypteret dele af din data.

Er de først inde i systemet, har de mulighed for at lære netværkets strukturer at kende, og gradvist udvide deres rettigheder for til sidst at opnå administratorstatus. Sker dette, kan hackeren tilgå alle informationer på dit netværk, og sågar slette eventuelle sikkerhedskopier af dine data. Her kan de for alvor gøre skade på din forretning.



Kilde: smvdanmark.dk/analyser



af alle virksomheder mangler udførlige sikkerhedsprocedurer og handlingsplaner, der kan aktiveres i tilfælde af cyberangreb.

2 Phishing

Phishing er et af de mest almindelige ransomware-angreb. Phishing går i al sin enkelthed ud på, at hackeren forsøger at få adgang til informationer, systemer eller netværk ved at udgive sig for at være en intern medarbejder eller kollega. Selvom de fleste er overbeviste om, at de aldrig ville falde for sådan et forsøg, er både Google, Snapchat og Facebook eksempler på, at det kan ske for alle.
Cyberkriminelle er blevet eksperter i at gengive de rette menneskelige interaktionskriterier, og de ved, hvilke følelser, der virker. Phishing kan være så simpelt som en hacker, der udgiver sig for at være din kollega, og sender et link til et møde eller en email med nye opdateringer, der viser sig at være malware.

Tilgængeligheden af AI-værktøjer som ChatGPT og Wall-E har også gjort det sværere for cybersikkerhedsfolk at opsnappe forsøg på indtrængen. Disse værktøjer har gjort det muligt for enhver at sende sofistikerede og overbevisende emails, og skabe ondsindet kode uden at have den mindste form for teknisk ekspertise.

3 Insiders

Den menneskelige faktor udgør altid en risiko i en virksomhed. Ofte forekommer denne type angreb, når cyberkriminelle sender emails til medarbejdere i håb om at finde en person, der er villig til at hjælpe dem med at tilgå interne filer mod at få en større sum kryptovaluta som betaling.

Det tillokkende for medarbejderen er, at det hele foregår digitalt, og at det derfor ikke er nødvendigt at have direkte kontakt med hackeren. Det er netop af denne årsag, at alle virksomheder, udover at have de rette tekniske løsninger, også bør have en stærk, intern sikkerhedskultur med opstillede retningslinjer for rapportering af sikkerhedsbrister eller forsøg på indtrængen.

Omkring 80 procent af alle databrister involverer et menneskeligt element i en eller anden grad. Det er derfor vigtigt, at virksomheder holder sig opdaterede på udviklingen af cyberkriminalitet, så de kan undervise medarbejdere og implementere de rette foranstaltninger.

9 råd til bedre sikkerhed

For at beskytte din virksomhed mod ransomware-angrebenes ødelæggende konsekvenser er det nødvendigt at arbejde risikobaseret og forebyggende ud fra din virksomheds konkrete struktur. Det langsigtede mål er, gennem de rette værktøjer og rutiner, at opbygge et sikkert, fleksibelt og stabilt IT-miljø, der er i stand til opsnappe og respondere på angrebsforsøg.

Her får du ni generelle råd til, hvor du kan øge sikkerheden i din virksomhed, og blive bedre til at forhindre gennemtrængende angreb og tyveri.

1 Regelmæssige opgørelser

Infrastrukturen i en virksomhed vokser som regel proportionelt med antallet af leveår. Ofte vil vi se mere og mere komplekse løsninger, og det kan være svært at bevare overblikket over det samlede IT-miljø.

Vi anbefaler derfor altid, at man etablerer en ramme for regelmæssige opgørelser, hvor I gennemgår anvendte systemer, software og tjenester i organisationen, og ser på, hvilke personer, der har hvilke adgange.

Dette løbende opgørelsesarbejde bør være en naturlig del af den langsigtede IT lifecycle management. Dette inkluderer også at sørge for, at alle systemer er opdaterede, så eventuelle sårbarheder som leverandøren opdager kan blive fikset og lukket.

2 Minimering af angrebsfladen

En anden vigtig foranstaltning at tage, er at begrænse virksomhedens angrebsflade så meget som muligt. En angrebsflade kan være alle steder, hvor angribere kan få adgang – lige fra fysiske enheder, såsom computere og printere, til lagrede filer i skyen.

Den hyppige opgørelse som vi netop omtalte i afsnittet ovenfor, er central for at kunne gennemføre dette trin. Medarbejdere kan også være mulige "angrebsflader", og derfor kan det være en god idé at se nærmere på informationshierakiet i virksomheden, og begrænse deling af følsomme oplysninger blandt medarbejderne.

3 MFA (Multifactor Authentication)

Multifaktorgodkendelse er et effektivt værktøj til at sikre, at rette medarbejdere får adgang til de relevante data. Det har længe været almindeligt med tofaktorgodkendelse via sms, app eller email, men med MFA tilføres der et ekstra lag af beskyttelse ved at tilføre et eller flere trin til processen. F.eks. ved både at godkende med privat kode, kode på sms og biometri.
Etablering af flere faktorer i godkendelsesprocessen hjælper dig med at holde overblik over, hvem der har adgang til vigtige data, og samtidig er det ekstra lag af beskyttelse især vigtigt i virksomheder, hvor medarbejderne arbejder udenfor virksomhedens lokationer.

4 Login uden adgangskode

De fleste vil nok nikke genkendende til, at det kan være svært at huske meget komplicerede adgangskoder. Derfor vil vi ofte støde på, at medarbejdere har samme adgangskode til virksomhedens følsomme oplysninger, som de har til mange af deres private konti, og det er naturligvis ikke den bedste sikkerhedsforanstaltning mod cyberangreb.

Istedet er det bedre, at sikre en "kodefri" loginprocedure i virksomheden. "Kodefri" betyder ikke, at der ikke må eksistere koder i loginflowet, men det kan være en fordel at benytte autogenererede, unikke koder sammen med godkendelse via andre metoder, såsom app eller biometri. På denne måde kan I nedsætte risikoen for menneskelige fejl, når medarbejderne håndterer kritiske data.

5 Separate brugerprofiler

Hos de få i din virksomhed der besidder administratorrettigheder til kritisk data og følsomme oplysninger, vil det give øget sikkerhed, hvis disse brugeradgange kun benyttes, når det er allermest nødvendigt. I den resterende tid bør administatorerne have brugerprofiler med rettigheder, der fungerer til hverdagens opgaver. Ved at segregere identiteter på denne måde mindsker du risikoen for, at administratorrettigheder lander i de forkerte hænder.

6 Segregerede netværk

Hvis din virksomhed bruger flere forskellige netværk, kan det give et ekstra værn mod cyberangreb, hvis du segregerer, eller adskiller, virksomhedens netværk. Ved at holde dem adskilte mindsker du den potentielle rækkevidde af et eventuelt ransomware-angreb.
Det kan lyde kompliceret, men med rette hjælp kan processen lettes betydeligt. Det er desværre den skinbarlige sandhed, at jo mere simpel administrationen i din virksomhed er, desto lettere er den at overtage for en hacker.

7 Sikkerhedskopierede backups

Det kan måske umiddelbart virke som et råd, der giver sig selv, men det kan godt tåle at blive sagt igen; lav sikkerhedskopierede backups af al din data, men husk at fordele den kritiske data på flere forskellige backupsteder. Det er vigtigt, at al kritisk data ikke er tilgængeligt via samme backup, for det kan sætte din virksomhed i en mere sårbar position. Det kan f.eks. være en god idé både at have et flere tilgængelige online, og et flere offline-versioner, og sørg derudover for at implementere en intern backup-procedure, der udføres med jævne intervaller.

8 EDR-system – og kompetente medarbejdere

Det er ikke nok kun at monitorere og tracke aktivitet indenfor kontorets åbningstider. EDR står for Endpoint Detection and Response, og er en avanceret cybersikkerhedsteknologi designet til at identificere og respondere på ondsindet aktivitet på slutpunktsenheder, som f.eks. en telefon, computer eller tablet – i realtid, hele døgnet.
Ved hjælp af AI kan potentiel fare opfanges og rapporteres, og i nogle tilfælde afhjælpes. Det er dog vigtigt, at der er kyndige mennesker til at modtage rapporteringerne, så de kan vurdere den reelle risiko og foretage passende initiativer.

9 Patching

Sidst, men ikke mindst: lap, eller patch, eventuelle huller i sikkerheden, så snart de bliver opdaget. Virksomhederne er ikke de eneste, der har fået et ekstra værktøj i AI-teknologier – det har de cyberkriminelle også. Det betyder, at det er lettere end nogensinde at identificere aktuelle brister og sårbarheder i din sikkerhed. Sørg derfor for at have de rette værktøjer og procedurer på plads, så din vinduet til din virksomheds sårbarheder er åbent i så begrænset en mængde tid som overhovedet muligt.

Opsummering

01 Regelmæssige opgørelser

Foretag regelmæssige opgørelser over jeres systemer, databaser og tjenester , og sørg for at opdatere jævnligt, så eventuelle huller i sikkerheden bliver lukket med det samme.

02 Minimering af angrebsfladen

Sørg for at begrænse antallet af steder, hvor de følsomme data er tilgængelige, herunder også antallet af medarbejdere, der har adgang. Det minimerer antallet af indgange for hackere.

03 MFA (Multifaktorgodkendelse)

Hvis du fortsat benytter tofaktorgodkendelse for at sikre dine data, anbefaler vi, at du opgraderer, og inkluderer flere trin i godkendelsesprocessen for at tilføre et ekstra lag af beskyttelse.

04 Adgangskodefri loginprocedure

Implementér autogenererede koder, biometri eller godkendelse via tredjeparts-applikationer for at undgå, at dine medarbejder har samme kode på arbejdet, som de har til deres private data.

05 Segregerede identiteter

Opret adskilte brugere til de medarbejdere, der også har administratorrettigheder. På den måde minimere du risikoen for at administratorrettigheder lander i de forkerte hænder.

06 Segregerede netværk

Ved at adskille dine netværk styrker du værnet mod hackere. En simpel administration er ofte lettere at tvinge sig adgang til, og adskilte netværk sørger for at komplicere hackerens arbejde.

07 Sikkerkopierede backups

Sikkerhedskopiér dine backups, og sørg for ikke at have al dataen liggende samme sted. Gør det til en vane at sikkerhedskopiere dine data regelmæssigt, og placér det både online og offline.

08 EDR-system – og kompetent personale

Optimér overvågning og rapportering af ondsindet trafik ved at opsætte et EDR-system. Sørg dog altid for at have kompetente folk til at vurdere den reelle risiko af trafikken.

09 Patching

Sørg for at have de rette værktøjer og procedurer på plads, så din virksomhed kan handle hurtigt og lukke sikkerhedshullerne så snart de opdages.

Har I en sikkerhedsplan?

Har I en tilstrækkelig sikkerhedsplan på plads i jeres virksomhed, så I står stærkt mod de cyberangreb og sikkerhedsbrister, der truer virksomheder verden over?

Vi kan hjælpe med at implementere en ABC-cybersikkerhedsplan, som beskytter følsomme data mod tyveri, tab eller skade. Vi udvikler altid individuelt tilpassede sikkerhedsløsning designet til jeres specifikke behov og interne strukturer.

A

Hold de cyberkriminelle ude

Vi tilbyder en avanceret sikkerhedspakke, der identificerer og beskytter jeres netværk mod udefrakommende trusler.

B

Hold øje

Vi overvåger dit netværk og IT-miljø hele døgnet for at identificere og reagere på eventuelle sikkerhedstrusler.

C

Hav en backup-plan

Hvis uheldet er ude, skal I have en backup-plan. Vi har et dedikeret team af specialister, som proaktivt sikrer backup af jeres data.

Få et sikret netværk hos GlobalConnect

Få én samlet, sikret og beskyttet totalløsning, og forbind al din data på tværs af fysiske og digitale lokationer.
Fra fiber i jorden til data i skyen kan vi skræddersy et fleksibelt, skalérbart og fremtidssikret netværkdesign.

Læs mere på www.globalconnect.dk

GlobalConnect A/S

Havneholmen 6

2450 København SV

CVR 26759722

+45 77303000