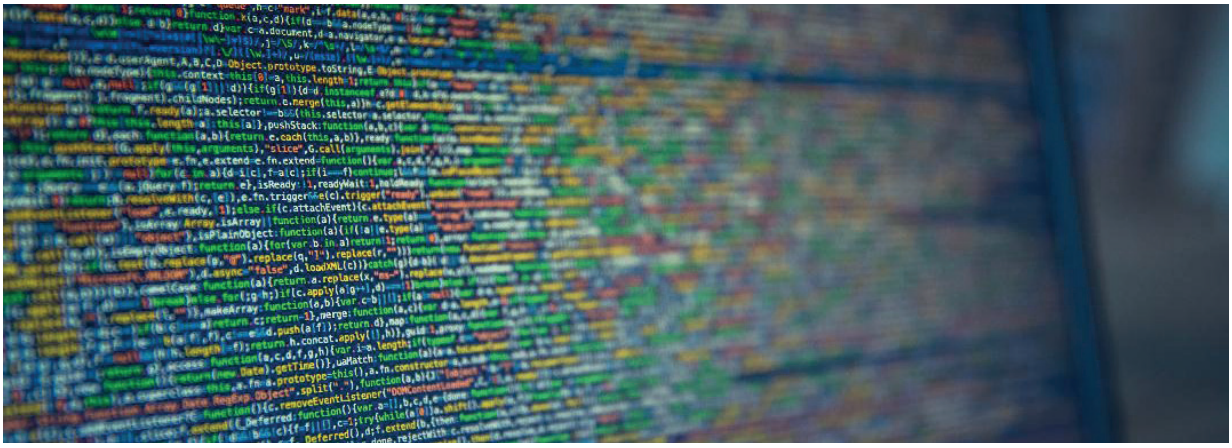
EZENTA BESKYTTER DANSKE VIRKSOMHEDER

Ezenta er en af Nordens førende it-sikkerhedsvirksomheder og leverer rådgivning og totalløsninger inden for området. Med afsæt i medarbejdernes dybe forståelse, erfaring og stærke kompetencer inden for it-sikkerhed samt partneraftaler med branchens absolut førende producenter af it-sikkerhed, hjælper Ezenta kunderne med at skabe sikre rammer omkring it – både i forbindelse med rådgivning, implementering og vedligeholdelse af sikkerheden.



Virksomheder er forskellige og har derfor også forskellige it-sikkerhedsbehov. Både Ezenta og Check Point Software Technologies, som Ezenta har været partner for siden 2000, fokuserer 100 procent på it-sikkerhed og forstår området på alle niveauer. Ezenta kan med de dybeste kompetencer løfte hver en sten hos kunderne og finde frem til de rette løsninger, mens Check Point har produkterne til at komme hele vejen rundt. Med udgangspunkt i Check Points produkter løfter Ezenta kundernes it-sikkerhed op på det niveau, den skal være på.

Trusselsbilledet er mere dynamisk end nogensinde før, og virksomheder forandrer sig endvidere konstant. Malware kan sprede sig og inficere adskillelige virksomheder på meget kort tid. Lægger man dertil, at truslerne er blevet langt mere avancerede, og at bagmændene er blevet betragteligt mere strukturerede og kyndige, står det klart, at cyberangreb udgør en langt større og mere alvorlig trussel mod virksomheders forretning end tidligere. Derfor er det vigtigt at få vurderet og testet it-sikkerhedsniveauet jævnligt. Ezenta hjælper med at give et holistisk billede på sikkerhedssituationen med henblik på at etablere et stærkt cyberforsvar og implementere de rette processer til at begrænse skaderne ved et sikkerhedsbrud.

Et sikkert netværk
Der er en konstant fare for, at cyberkriminelle angriber virksomheders netværk. Uden den rette beskyttelse af netværket giver man cyberkriminelle mulighed for at spionere, stjæle værdifulde data eller f.eks. lægge netværket ned med et DDoS-angreb. Og er de cyberkriminelle først inde, kan det være svært at finde dem. I gennemsnit tager det 180 dage

> **En god firewall analyserer trafikken og beskytter netværket mod allerede kendte sårbarheder.**

for virksomheder at finde ud af, at de er blevet kompromitterede. Det kan have enorme konsekvenser for virksomhedens bundlinje, oppetid, konkurrenceevne og ikke mindst omdømme. Derfor er det essentielt at have en god it-sikkerhedsløsning, som kombinerer en modstandsdygtig Next Generation Firewall med en effektiv sandboxing-løsning og det rette sikkerhedsudstyr.

En god firewall analyserer trafikken og beskytter netværket mod allerede kendte sårbarheder. Den kontrollerer også, hvordan brugere anvender virksomhedens programmer ved at identificere brugeren og sætte de rette begrænsninger eller endda blokere for adgang. Ydermere giver en god firewall mulighed for at styre, hvilke apps der bliver brugt i virksomhedens netværk. En firewall med disse funktioner giver både ledelse og it-sikkerhedsmedarbejdere ro i sindet, fordi de kan gardere sig mod kendte trusler og styre hvilke personer og programmer, der skal have adgang til virksomhedens dyrebare data.

Fordelen ved at supplere en god firewall med en effektiv sandbox-løsning er, at sandboxing beskytter virksomheder mod ukendt malware og målrettede angreb ved at emulere ukendte filer og sætte en stopper for potentielle angreb, før de får mulighed for at komme ind på netværket. Her er det afgørende, at løsningen analyserer så mange filtyper som muligt, da de cyberkriminelle typisk forsøger sig med mange forskellige filtyper, når de angriber virksomheder via e-mails, downloads eller hjemmesider. Check Point har den løsning, som beskytter flest filtyper og dermed dækker bredest. Med effektiv sandboxing kan ledelse og it-sikkerhedsmedarbejdere få vished om, at kun sikkert indhold bliver delt med brugerne af netværket.

Check Points løsninger inden for netværkssikkerhed:
- Sandblast Network med beskyttelse på CPU-niveau, som understøtter over 40 filformater
- Next Generation Firewall med identity awareness, IPS detection og application control
- Security Gateway Appliances med mulighed for VPN-forbindelse, antivirus, anti-bot, anti-spam mm.

Medarbejderne er det svageste led

Medarbejdere er og bliver en stor svaghed i virksomheders it-sikkerhedsindsats. Dels fordi de med deres begrænsede viden om truslerne i cyberspace er nemme ofre, hvilket gør virksomheder sårbare over for phishing-angreb og malware, som kan resultere i, at værdifulde informationer bliver stjålet eller slettet. Og dels fordi, de er langt mere mobile end tidligere, hvilket resulterer i, at laptops ofte opererer uden for virksomhedens (måske) ellers sikre netværk. Det giver cyberkriminelle mulighed for at få adgang til sensitive data eller de kan få succes med ransomware-angreb, hvor de afpresser økonomisk via kryptering eller trusler om at frigive sensitive informationer.

> **En VPN-forbindelse kan give medarbejdere på farten sikker adgang til virksomhedens netværk og dermed sikker adgang til arbejdsrelaterede data.**

De cyberkriminelle er mere end klar over, at medarbejderne ofte udgør det svageste led i virksomheders it-sikkerhed, og det udnytter de til at få en bagdør ind i virksomheders netværk. Derfor er det vigtigt at have it-sikkerhedspolitikker som betyder, at medarbejderne agerer sikkert. Mange virksomheder er gode til at få implementeret it-sikkerhedspolitikker, men desværre er der også mange, som ikke håndhæver dem. Derfor kan det være en stor hjælp at få teknisk understøttelse af reglerne. Man bør sørge for at have en løsning, som fra centralt hold giver mulighed for at sikre, at medarbejderne lever op til reglerne på virksomhedens netværk; at de rette sikkerhedsprodukter er installeret og opdateret; at endpoint-maskinerne kører det korrekte operativsystem; og at medarbejderne kun kan køre godkendte applikationer på deres maskiner. På den måde minimerer man risikoen for, at medarbejderne uforvarende lukker cyberkriminelle indenfor.

En VPN-forbindelse kan give medarbejdere på farten sikker adgang til virksomhedens netværk og dermed sikker adgang til arbejdsrelaterede data. Her er det en fordel at sørge for en VPN-løsning, som har en god brugeroplevelse, fordi det giver medarbejderne større mulighed for at komme hurtigt i gang med deres arbejde. For at styrke endpoint-sikkerheden er det også en god ide for virksomheder at udvide deres zero-day-beskyttelse, så medarbejderne er beskyttet mod avancerede angreb – selv på farten. En god end-point-løsning sender bl.a. filer til inspektion i en virtuel sandbox, hvilket forhindrer malware og ransomware i at nå frem til brugeren. Skulle en usikker fil slippe igennem, er det vigtigt at have en teknologi på plads, som inddæmmer skaden. En god endpoint-løsning genererer automatisk hændelsesrapport om entry points, omfanget af skaden og inficerede maskiner, så de it-sikkerhedsansvarlige hurtigt kan løse sikkerhedshændelser, og med-arbejderne kan fokusere på deres arbejde – til glæde for medarbejderne selv men også for forretningen.

CheckPoints løsninger inden for endpoint-sikkerhed:

- Endpoint Policy Management
- Sandblast Agent med trusselsemulering, Threat Extraction, Anti-Ransomware, Anti-Bot, Zero Phishing and Automated Incident Analysis
- Endpoint Remote Access VPN Software

Sikkerhed i skyen

Selvom virksomheder kan effektivisere forretningsprocesser ved at køre tjenester i skyen eller ved at lægge dele af eller hele infrastrukturen i skyen, er det også forbundet med en række nye udfordringer, som relaterer sig til it-sikkerhed. Det er blandt andet meget udbredt, at cyberkriminelle tiltusker sig adgang til virksomhedens ellers godt beskyttede

> **Mange virksomheder kæmper med at overføre deres ofte gode it-sikkerhedsmodel til skyen.**

netværk via phishing mails i Office365, som narrer brugeren til at udlevere sit brugernavn og adgangskode – eller endda finansielle oplysninger. En cyberkriminel kan for eksempel udgive sig for at være den administrerende direktør og bede en medarbejder om at overføre penge til sin egen konto. Fænomenet hedder CEO-fraud og adskillelige cyberkriminelle er sluppet godt afsted med at udføre det med meget store beløb som uberettigede gevinster.

Mange virksomheder kæmper med at overføre deres ofte gode it-sikkerhedsmodel til skyen. For uanset om der er tale om SaaS, offentlig IaaS eller privat IaaS er et sikkerhedsbrist hos leverandøren ensbetydende med et sikkerhedsbrist hos den virksomhed, som har lagt sine data i leverandørens cloud. Derudover åbner de evigt nye cloud-tjenester op for nye muligheder for skygge-it blandt medarbejderne. Dermed bliver håndhævelse af it-sikkerhedspolitikker relevant igen, for medarbejdernes brug af skygge-it kan resultere i, at virksomheden får tjenester ind i netværket, som ikke er sikret optimalt – og på den måde sætter man sine værdifulde informationer over styr.

Når man opererer med tjenester som Dropbox, Office 365 eller Slack, er det nødvendigt at sætte sin it-sikkerhed op, så den beskytter virksomheden mod ukendte trusler og phishing mails. Man skal blokere for adgang til ukendte brugere og kompromitterede enheder og beskytter data ved blandt andet at blokere for deling af sensitive data og ved at identificere og kontrollere skygge-it. Når man lægger sin infrastruktur i skyen – uanset om man har lagt den i en public eller private cloud – handler det om at finde en it-sikkerhedsløsning, som følger de gode takter, som en Next Generation firewall og

sandboxing kan tilbyde. Med disse avancerede løsninger, sørger man for, at data ikke falder i de forkerte hænder, selvom skyen giver adgang til virksomhedens forretningshemmeligheder, persondata, immaterielle rettigheder eller andre sensitive informationer.

Check Points løsninger inden for cloud-sikkerhed:
- CloudGuard SaaS
- CloudGuard Public IaaS Security
- CloudGuard Private IaaS Security

Vi er blevet mere mobile

Medarbejdere er blevet langt mere mobile end tidligere, og de fleste har fortrolige firmadata på deres smartphones og andre enheder. Særligt på mobile enheder er linjerne mellem privatlivet og arbejdspladsen slørede. Der skal dog ikke herske tvivl om, at mobile enheder er en potentiel bagdør til virksomhedens netværk. Denne bagdør gør cyberkriminelle i stand til at stjæle værdifulde informationer eller følge med i, hvad medarbejderne foretager sig. Cyberkriminelle kan blandt andet komme ind på mobile enheder via ondsindede apps, åbne Wi-Fi-netværk, sårbarheder i operativsystemerne eller ved at sende ondsindede links i SMS-beskeder. Alligevel er der mange virksomheder, som ikke prioriterer sikkerheden tilstrækkeligt på dette område.

> **Når en medarbejder bruger en enhed til både private og professionelle aktiviteter, er det en god ide at finde en løsning, som adskiller forretningsinformationer fra personlige informationer**

For at sikre de mobile enheder bedst muligt er det vigtigt at lede efter en løsning, som beskytter i flere lag. Den skal beskytte mod apps med malware, man-in-the-middle-angreb via Wi-Fi, farlige links via SMS, ukendte sårbarheder og kendte sårbarheder i operativsystemet. En god løsning sætter en inficeret enhed i karantæne og udelukker den fra netværket så længe den registrerer en trussel. Check Points mobilløsning er den eneste på markedet, som beskytter på alle områderne. Desuden kan it-sikkerhedsmedarbejdere få overblik over de mobile trusler, fordi løsningen sender data til dem. De kan derfor følge med i sikkerhedshændelser i realtid og træde ind med det samme, hvis det skulle være nødvendigt. Og de kan se, hvor mange mobile trusler, virksomheden står over for, samt hvilke trusler, der dominerer trusselsbilledet. Det giver selvfølgelig et overblik over truslerne mod virksomheden, som den kan bruge til at tage de nødvendige forholdsregler – såsom tilpasning af it-sikkerhedspolitikker – for at beskytte virksomhedens værdifulde data.

Når en medarbejder bruger en enhed til både private og professionelle aktiviteter, er det en god ide at finde en løsning, som adskiller forretningsinformationer fra personlige informationer ved at kryptere data, så de kun når frem til autoriserede brugere. Desuden skal man kunne slette enheden fra centralt hold, hvis den bliver væk eller bliver stjålet, og sørge for, at kun sikre enheder kan få adgang til informationerne. Medarbejderne kan således få fjernadgang til e-mail, kalender, dokumenter eller tjenester, selvom de ikke befinder sig i virksomhedens netværk, hvilket gør dem i stand til at arbejde fra enheden hvor som helst og helt ubekymrede. Samtidig kan ledelse og it-sikkerhedsansatte få ro i sindet, fordi informationerne forbliver beskyttede både i virksomhedens netværk og udenfor.

CheckPoints løsninger inden for mobilsikkerhed:
- Sandblast Mobile
- Capsule Workspace

Kompleksiteten stiger

I takt med at virksomheders netværk bliver større, antallet af forskellige enheder vokser og flere forskellige teknologier kommer i brug bliver trusselsbilledet og it-sikkerhedsindsatsen også langt mere kompleks. Derfor er det essentielt med en løsning, som hurtigt kan skabe overblik, så man undgår at hyre en skov af it-sikkerhedsfolk for at have et overblik over de forskellige trusler, der er på tværs af netværk, cloud-tjenester og mobile enheder. Ydermere ligger der i GDPR, at virksomheder skal have et passende sikkerhedsniveau, hvilket gør et overblik endnu vigtigere end tidligere. Der er nemlig alvorlige økonomiske sanktioner forbundet med ikke at leve op til GDPR.

> **Det sparer virksomheder både tid og penge og gør det nemmere at leve op til EU-persondataforordningen.**

For at få overblik skal løsningen samle alle sikkerhedsprotokoller, -funktioner og -politikker ét sted. Det giver nemlig virksomheder mulighed for nemt at styre it-sikkerhedsprodukterne og sørge for sammenhæng på tværs af it-infrastrukturen. Og det giver dem også mulighed for at skabe, tilpasse og overvåge it-sikkerhedspolitikker på tværs af brugere, enheder, applikationer, data og netværk. Det er desuden en fordel, at løsningen automatiserer rutinemæssige opgaver, så it-sikkerhedsmedarbejderne kan dedikere deres tid til håndtering af sikkerhedshændelser. Her er det nødvendigt med en løsning, som giver fuld synlighed over truslerne og mulighed for at undersøge hændelserne i realtid, så it-sikkerhedsafdelingen kan tage kontrol over indsatsen og reagere på hændelser med det samme.

Kort sagt skal løsningen tage en masse data fra alle interne hændelser og eksterne hændelser for at give et samlet og retvisende trusselsbillede og koge det ned til et overskueligt format, så både it-sikkerhedsafdelingen og ledelsen kan få overblik over de mage komplekse data – og dermed indblik i virksomhedens it-sikkerhedsindsats over for trusselsbilledet. Det sparer virksomheder både tid og penge og gør det nemmere at leve op til EU-persondataforordningen.

Check Points unikke løsninger inden for Security Management:

- Security Management/Infinity
- Next-Generation SmartEvent
- Security Management Appliances