Managed Detection & Response:

Adfærd og overblik er alfa og omega inden for it-sikkerhed – men hvordan skaffer man sig det?

Et sted, der altid er aktivitet, er på it-sikkerhedsområdet. Det er uoverskueligt at følge med i de it-kriminelles aktiviteter, men det er mindst lige så uoverskueligt at følge med i de nyeste løsninger og teknologier, der findes på markedet for sikker it. Desværre er det ikke gjort med at holde sig ajour på de områder, for et faktum er, at den største trussel mod din virksomheds it-sikkerhed er medarbejdernes adfærd. Opgaven at sikre sit it-system har mange facetter, og et godt sted at begynde er at kigge på udfordringerne, men kan man kombinere sine eksisterende sikkerhedsløsninger og derved opnå et samlet overblik, er man godt på vej.

UDFORDRINGER OG TRUSLER

Typiske reaktionsmønstre ved hacker-angreb

Vil du bevare overblikket og hurtigt få identificeret årsagen til angrebet og isoleret den eller de angrebne enheder? Eller er det mere sandsynligt, at du vil blive grebet af panik og gribe til en irrationel handling? Mange gribes af panik og handler på en ikke særlig gennemtænkt måde, når vi bliver udsat for et hacker-angreb. Hos Ezenta, der dagligt arbejder med it-sikkerhed, oplever vi stort set alle typer af adfærd. Nogle, hvor reaktionen er mere skadelig end selve hændelsen. Nogle begynder at reetablere deres systemer med data fra en tidligere backup og mister dermed alle de mellemliggende data. Andre bruger uforholdsmæssigt meget tid på at finde ud af, hvordan angrebet kunne ske. Endelig er der de mange, som slet ikke reagerer, fordi de ikke er klar over, at de har været udsat for et angreb. Måske får de det at vide fra en ekstern kilde. Måske får de det aldrig at vide.

Fælles for de ovennævnte reaktionsmønstre er, at de lugter langt væk af panik, og de er ikke optimale for virksomhedens forretning og it-drift fremadrettet.

> **Det handler om at være klædt på til at planlægge og beskytte, at opdage og identificere, og endelig om at reagere på den mest fornuftige måde.**

Analyse og planlægning
Ingen kan beskytte sig 100 procent mod alle trusler, og der findes ikke én teknologi eller løsning, som kan spærre for alle angreb og lukke alle trusler ude. Og ingen kan realistisk beskytte alle sine data. Derfor handler det om at analysere sit behov og gradbøje begrebet 'kritisk'. Hvilke data og sårbarheder er mest kritiske eller fatale for virksomheden og må for enhver pris hverken mistes eller blive kompromitteret? Disse data og sårbarheder skal naturligvis have topprioritet og sikres med tilstrækkelige midler. I den anden ende af skalaen kan man måske bedre tillade sig at vurdere ud fra de omkostninger, der er forbundet med sikring og holde dem op imod de økonomiske konsekvenser et vellykket hackerangreb vil have.

Opdag og identificér!
Det er slemt at opdage, at man er blevet angrebet af cyber-kriminelle og for eksempel har mistet data. Men det er værre at være angrebet og IKKE opdage det. Det sker desværre ofte, at virksomheders it-system er blevet angrebet og måske endda stadig fungerer som vært for ondsindet virus, uden at det er blevet opdaget. Derfor bør man med jævne mellemrum få testet sine it-systemer for sårbarheder. Den teknologiske udvikling på cyber crime-området sker med lynets hast, og trusselsbilledet ændrer sig konstant. At holde sig opdateret på it-sikkerhedsområdet er et fuldtids job, som mange organisationer ikke selv har ressourcerne til. Derfor kan det være hensigtsmæssigt at vælge ekstern hjælp.

Det er vigtigt at vide præcis, hvad de cyber-kriminelle er ude efter, hvordan de tænker, og hvilke sårbarheder de sigter mod lige nu. Det er meget svært - for ikke at sige umuligt at være et skridt foran. Med mindre man kender hacker-miljøet. Rapid7, som er den software-producent, Ezenta baserer sin sikkerhedsløsning Managed Detection and Response på, udvikler også den software mange hackere bruger. Det vil sige, at ingen kender hackernes metoder og adfærd bedre end Rapid7. Det giver naturligvis et stort forspring i forhold til at være up to date og på forkant med situationen.

Den fornuftige reaktion
Tilbage til vores adfærd, og hvordan vi reagerer i pressede situationer. Der er ingen tvivl om, at de fleste af os ikke reagerer hensigtsmæssigt, når vi bliver presset. Men man kan øve sig og blive bedre til at håndtere kriser. Men hvem har råd til at øve sig, når det handler om it-sikkerhed? Korrekt håndtering af cyber-angreb handler i høj grad om at skabe den rette kultur i virksomheden. Der bør være en åben og ærlig kultur, hvor medarbejderne tør spørge og fortælle, hvis de er kommet til at begå en fejl. Ingen er tjent med, at medarbejdere skjuler fejl og bommerter. Men det er desværre en naturlig reaktion, hvis virksomheden ikke har en fornuftig og brugbar sikkerhedspolitik. Hvem ønsker åbenlyst at indrømme, at man har begået en fejl? Man har endda hørt om virksomheder, der afskediger medarbejdere, som er kommet til at forårsage et brud. Når man vælger at bruge tid på at identificere sårbarheder og årsag, så risikerer man at skabe en atmosfære af frygt blandt medarbejderne. Og man risikerer også, at angrebet derfor spredes unødvendigt, hvor man i stedet kunne have brugt tiden på at standse det.

Tag nu for eksempel din egen virksomhed. Hvad skete der sidst den blev ramt af et cyber-angreb? Kan du forklare og dokumentere angrebet?

> **Hvis du har mistet personhenførbare data, skal du ifølge GDPR-lovgivningen inden for 72 timer efter bruddet kunne dokumentere en række ting, blandt andet hvor mange personer og hvilke data, der er berørt.**

Du skal desuden kunne beskrive, hvordan bruddet er foregået, og hvilke konsekvenser, det kan få, og sidst men ikke mindst, skal du kunne redegøre for, hvad I har gjort for at rette op på bruddet. 72 timer er rigeligt med tid, hvis der er overblik over enheder, dataflow og sårbarheder. Men hvis det ikke er tilfældet, er 72 timer ingen tid. Det er her en MDR-løsning kan bevise sin værdi.

MANAGED DETECTION AND RESPONSE

Hvad er en MDR-løsning?
I erkendelsen af at der ikke findes én teknologi, som kan lukke for alle trusler, og at det er et fuldtidsjob at holde sig ajour med det aktuelle trusselsbillede, så vælger mange at få ekstern hjælp. Hjælp til at skaffe sig overblik over enheder og flows i organisationen. Og hjælp til at få indsigt i trusler og løsninger. Ezenta har udviklet en MDR-løsning, der matcher disse behov. Ezentas MDR-løsning er en managed service løsning, der indeholder alle de elementer, der er væsentlige for sikker it. Det vil sige monitorering, rådgivning, uddannelse, analyse og test. Qua vores it-sikkerhedseksperter råder Ezenta over mange års erfaring og specialistviden. Teknologien bag vores løsning leveres af Rapid7, som er en af markedets førende leverandører på dette område.

En MDR-løsning er en række af tjenester, som vi sammensætter i samarbejde med dig, så løsningen matcher din virksomheds situation og behov. Vi implementerer UEBA (User Entity Behavoir Analytics) og ABA (Attack Behavior Analytics) hos dig, så vi kan opsamle og monitorere informationer om aktuelle angreb og give dig besked, så du kan forhindre et succesfuldt angreb. På baggrund af de resultater, vi observerer, kan vi give dig et billede af, hvordan angreb typisk foregår, hvordan de håndteres, hvilke brugere og data, der har været berørt af et angreb og meget mere. Det er bl.a. vigtigt i GDPR-sammenhæng. I vores rådgivning til dig ligger en prioritering af vores anbefalinger. De vil blive inddelt i kategorier: High, medium og low efter hvor kritiske de er, hvordan og i hvilken rækkefølge de bør udbedres.

Sikkerhed omfatter også de eksterne enheder
Det er ikke alene vigtigt at kende situationen for enheder og systemer i virksomheden. I dag arbejder medarbejdere alle steder fra, og det er derfor mindst lige så vigtigt at kende til systemer og enheder, der ikke befinder sig inden for virksomhedens område. Derfor inkluderer Ezentas MDR-løsning også monitorering af enheder som computere og mobiltelefoner, der tages med uden for virksomhedens område. Det sker via implementering af en collector på enhederne. Collectoren vil monitorere brug af cloud-tjenester, Windows-miljøer og lignende. Computere der er blevet udstyret med en agent, vil konstant blive monitoreret for ændringer i adfærden og på den måde kan virksomheden få en advarsel om, at der muligvis bliver gjort forsøg på indtrængen via enheden.

På den måde får du et langt mere reelt overblik over it-infrastrukturen, og virksomhedens it-sikkerhed øges væsentligt. Og hvis du har brug for hjælp til at løse udfordringerne og minimere risici, så står Ezentas CIRT (Computer Incident Response Team) til din rådighed.

Takket være vores samarbejde med Rapid7 er vores systemer altid opdaterede, og vi får tips om de nyeste angrebsmønstre, som Rapid7 indsamler hos efterretningstjenester over hele verden.

> **Når vi er opdateret, er du det også. Det skaber værdi for dig som bruger af vores MDR-løsning.**

En anden ting, der skaber værdi for vores kunder, er vores proaktive tilgang. Det er blandt andet denne proaktivitet, der har fået Gartner til at anerkende Ezenta som en af otte MDR-leverandører i Europa.

Proactivity-as-a-Service
Med en MDR-løsning kan du tilkøbe et abonnement på et antal audit-ydelser, test og rådgivning, som frit kan bruges inden for et år. Vi har inddelt ydelser i 3 kategorier: Ruby, Sapphire og Emerald. Du vælger selv, hvornår du mener, der er behov for at gennemføre de forskellige ydelser. Hvis du finder ud af, at du har mere brug for en ydelse i en anden kategori, end den du har valgt. Så kan du bytte den nye ydelse, du ønsker ud med en af dem, du har, så længe værdien for de to ydelser er den samme.

De tre kategorier ser således ud:

- **Ruby**
  En Ruby-audit er en mindre standardopgave og kan for eksempel være en test af om virksomhedens firewall eller pc-image har det forventede eller ønskede sikkerhedsniveau.

- **Sapphire**
  En Sapphire-audit er en mellemstor opgave. Det kan for eksempel være en penetrationstest af virksomhedens webapplikationer eller en phishing-kampagne, der kan måle organisationens modstandskraft overfor tilfældige eller målrettede angreb.

- **Emerald**
  En Emerald-audit er oftest et større projekt, der udføres i tæt samarbejde med kunden. Det kan for eksempel være en Awareness-kampagne eller en Red Team-opgave.

MANAGED DETECTION AND RESPONSE			
RAPID7 - IDR	Monitoring services		
EZENTA CIRT	Incident Response Service		
OPTIONS	**Ruby** Perimeter scan Client Assessment Firewall Assessment Wireless Assessment Townhall meetings	**Sapphire** Web penetration test ACE course Phising attacks Vulnerabillity Assessment	**Emerald** Attack simulation Awareness for users

VÆRDIEN AF EN MDR-LØSNING

For en moderne virksomhed er velfungerende it lige så vigtig som rent drikkevand for en kommunes borgere. Cyber-kriminaliteten er stigende og har været det længe. Derfor er it-sikkerhed en absolut nødvendighed, der skal prioriteres. Det kan naturligvis gøres på mange måder, men faktum er, at hvis der skal være kvalitet bag sikkerhedsløsningen, så kræver det, at der afsættes ressourcer – mange ressourcer. Mange organisationer hverken kan eller vil prioritere at afsætte tilstrækkelige ressourcer internt til it-sikkerhed. Det giver mere mening at benytte virksomhedens ressourcer til udvikling af nye it-projekter, der skal bidrage positivt til bundlinjen.

Det altoverskyggende formål med en MDR-løsning er derfor, at du kan sove roligt om natten. En MDR-løsning hos Ezenta giver dig det overblik over enheder, systemer og trusler, der gør at du føler dig tryg og kan have tillid til, at vi vil levere monitorering, respons, rådgivning og uddannelse, så din virksomheds it fungerer, som den skal, og ingen data går tabt eller bliver kompromitteret.

På det mere praktiske niveau kan en MDR-løsning nedsætte tiden fra et angreb bliver begået, til det bliver opdaget. Et tidsrum der kan have store konsekvenser for angrebets omfang. Erfaringer har vist, at en MDR-løsning typisk nedsætter tidsrummet, fra et angreb finder sted, til det bliver opdaget fra i gennemsnit 105 dage til ganske få timer – nogle gange kun minutter.

DET SIGER KUNDERNE

De arbejder i vores interesse

“Hackerne bliver hele tiden bedre og bedre, og vi er nødt til at følge med og bygge vores hegn højere. Vi har ikke en dedikeret ressource til it-sikkerhed, derfor bruger vi Ezenta til sparring og rådgivning inden for de fleste discipliner vedrørende it-sikkerhed. Både den forebyggende, men også hvis vi ser en trussel. Vi har et godt samarbejde med deres konsulenter, som hurtigt har forstået vores forretning og sat sig den ind i den ud fra et it-sikkerhedsmæssigt perspektiv. De er objektive og kommer her som troværdige rådgivere, der arbejder i vores interesse,” siger Claus Nybro, IT Driftchef, Semler Services om Ezentas MDR-løsning

Læs hele casen: https://www.ezenta.com/referencer/semler/