Cisco Partner
Gold Certified
Lifecycle Advisor

Så skyddar du dig när Internet blir mörkt!

April, 2020
Conscia Sverige Whitepaper

conscia

INNEHÅLL

Varför ska en organisation investera i säkerhet?

För många organisationer kanske svaret är självklart. Det är också rätt uppenbart för den som sett och upplevt många olika IT-miljöer att det ändå inte är så självklart i alla organisationer. Det är vanligt att säkerhetsmedvetandet fortfarande är lågt och därmed också förståelsen och viljan att investera i säkerhet. Det skiljer dock i branscher och olika marknadssegment.
IT-säkerhet är en fråga om att förstå men också att skydda de affärsmässiga värdena och ytterst hela verksamhetens existens. Att minimera risken att data raderas, förvanskas, stjäls eller görs oåtkomligt på något vis eller på andra vis ställer till det för verksamheten. Det också en fråga om att minimera skadeverkningar vid exempelvis en cyberattack. För att skydda sig behövs kunskap, processer och rutiner implementeras, verktyg i form av olika säkerhetssystem och lösningar samt en organisation för att ta hand om detta. Just det sistnämnda är ofta en utmaning i sig själv i tider där det inte är möjligt att rekrytera eller ens hitta de rätta kompetenserna att bemanna säkerhetsarbetet med.
Allt detta är kostsamt och det gäller att använda de ekonomiska resurserna där de gör störst verkan.

Lägg fokus på säkerhetshöjande system

Många av dagens cyberattacker är avancerade och det är svårt att skydda sig helt mot dessa. Det finns inget hundraprocentigt skydd och någon absolut säkerhet existerar inte. Det är en ständig katt- och råtta-lek mellan ”de goda” och ”de onda”.
Det blir ofta en balansgång mellan ökad säkerhet och investeringar som krävs för nå en ”tillräcklig” säkerhet.
Det betyder att för att skydda företages affärskritiska system och data behöver all säkerhet som rimligen kan, implementeras. Investeringar behöver utvärderas mellan nytta i förhållande till det skydd som erhålls. Detta är inget som är statiskt utan behöver revideras kontinuerligt då olika trender utvecklas och förändrar olika säkerhetssystems förmågor och effektivitet och därmed också hur investeringar bör göras inom IT-säkerhet.

”Internet is going dark”

Exempelvis kan en mega trend som ”Internet is going dark” medföra att effektiviteten i traditionella IPS/IDS system och brandväggar med applikationsfunktionalitet och tillhörande tjänsters effektivitet kommer att minska (eller i många fall redan har gjort). Svårigheten att se den riktiga applikationstrafiken när nästan all datatrafik mot Internet är krypterad är en trend som är känd sedan länge men ändå något som många valt att blunda för. Detta är något som är självförvållat i säkerhetsarbetet då det såklart är en god intention att införa kryptering. Det går förvisso fortfarande rent tekniskt att avkryptera viss krypterad trafik för inspektion i säkerhetssystem som IPS/IDS, applikations-brandväggar och URL-filter men det är besvärligt och kostnadsdrivande.

Många väljer därför att inte göra detta utan istället blir brandväggarnas primära uppgift att segmentera och eventuellt andra funktioner som kan åstadkommas utan att avkryptera applikationstrafik.
Tunga investeringar på applikations brandväggar, IPS/IDS bör kanske därför vägas mot andra skydd istället. Investeringarna som faktiskt gör mer nytta för den totala säkerheten. Traditionella brandväggar som användes innan applikationsbrandväggarnas intåg blir relevanta igen. Enklare brandväggshårdvara med mindre mjukvarufunktioner och licenser kanske kan användas. De ger mer potentiellt mer prestanda för en lägre kostnad. Resurser som kan användas till andra säkerhetshöjande system.

Säkerheten flyttar längre ut

På grund av att datatrafikens innehåll inte längre kommer att kunna läsas av säkerhetssystem måste mycket av säkerheten flytta längre ut och bli mer distribuerad. Säkerhet behöver förstärkas längst ut i serverar med tillhörande applikationer samt på klienter och övriga tillhörande stödsystem. Med andra ord i ändpunkterna där datatrafiken inte är krypterad bör säkerheten stärkas med bra klientsäkerhet, DNS skydd som komplement till klientskydd. Email-säkerhet behöver ligga på en hög nivå och moln-baserade säkerhetslösningar som skyddar de resurser och data som finns i molnet. Även system som kan detektera anomalier bör införas.

Ökat fokus på användarsäkerhet

De flesta företag har säkrat upp grundläggande användarsäkerhet med hjälp av lösenords-policys, elementär användarsäkerhet. Däremot är det många företag som saknar en förstärkt användarautentisering. Ett område där säkerheten ofta kan förstärkas och tillföra en väsentligt högre grad av säkerhet.
Multifaktor autentisering tillför extra säkerhet när övriga säkerhetssystem inte klarar uppgiften eller när en obehörig på något annat sätt lyckas få tillgång till en användares dator, inloggningsnamn samt lösenord.

En guide till säkerhetshöjande system

Exempel på säkerhetshöjande system och lösningar som bör övervägas och många gånger förbättras eller kompletteras är:

- **Klientskydd** – Ett bra klientsäkerhetsskydd är väldigt viktigt och det är en av de platser där oegentligheter har en möjlighet att upptäckas utan krypterings problematiken i nätverken. Klientskyddet bör samverka med andra system både preventivt men också ur ett responsperspektiv.
- **DNS-skydd för klienter** – Använd DNS-skydd som ett första linjens försvar som fungerar som komplement till klientsäkerhetsskydd. Det get en utökad klientsäkerhet samt medger delvis också viss kontroll över innehållsfilter baserat på domän-nivå.
- **Segmentering av nätverk** – Ett alltid giltigt skydd som minimerar skada vid eventuella cyberattacker samt förhindrar oönskad åtkomst av resurser.
- **Åtkomstkontroll av nätverk och resurser** – Åtkomstkontroll säkerställer att endast behöriga har den åtkomst de ska ha till nätverket och att de placeras i rätt segment i det segmenterade nätverket.
- **Förstärkt email säkerhet** – Email är fortfarande den absolut största attackvektorn. Både genom att farliga länkar distribueras via email men också skadlig kod som bifogas i email
- **Cloud-säkerhetsskydd** – Säkerställer skydd i och mot molnbaserade miljöer som olika typer av Software as a Service (SaaS) samt Infrastructure as a Service (IaaS).
- **System för att upptäcka anomalitet** – I och med att det är svårt eller omöjligt att göra inspektion i datapaketens innehåll i nätverket på grund av kryptering måste andra metoder användas. Att titta på beteende och mönster i kommunikation och detektera anomalier är ett skydd som kan hjälpa till med detta och bör övervägas
- **Molnbaserade ”Threat Intelligence” system** – Tillför inspektion av dynamiskt innehåll, dvs har förmåga att utvärdera ej tidigare känt innehåll som filer och på ett automatiserat sätt utvärdera om dessa är farliga eller ej och sedan distribuera detta vidare till andra system som kan dra nytta av detta i form av ”Threat intelligence” informations strömmar som kan abonneras på av olika säkerhetssystem.
- **”Threat Response” system**– Hot måste kunna detekteras snabbt och avvärjas på kortast möjliga tid. System som samverkar och kan nyttja automatisering blir viktigare än någonsin då skadlig kod relativt enkelt kan kryptera 10 tusentals datorer på mindre än 10 minuter. För att åtgärda sådana hot krävs automatisering och samverkande system. Mänskliga experter har helt enkelt inte möjlighet att åtgärda ett stort hot inom rimlig tid.

Dessa typer av skydd förväntas ta bort det flesta cyberattacker mot en IT-miljö, men det finns ingen garanti att inte någon attack faktiskt ”slinker” igenom, det är rentav sannolikt att någon tar sig igenom. Två parametrar som viktiga i sammanhanget är hotbild mot företaget och tid. Även om hotbild kan förväntas vara lägre mot ett företag så talar tidsaspekten emot. Det är inte frågan om utan när något sker. Även företag med låg hotbild råkar ut för allvarliga attacker.

Summering

Det har aldrig varit viktigare att fokusera på säkerhetsarbetet än nu och inget tyder på att det kommer minska utan snarare exponentiellt öka. I det avseende är det väldigt viktigt att investering i säkerhet görs där den gör mest nytta och att verkligen säkerställa att det blir så mycket säkerhetshöjande effekt som möjligt för de investeringar som behöver göras.
I en utveckling där applikationer kommunicerar krypterat och insynen minskar är det tydligt att säkerhetsarbetet och verktygen måste följa efter. Säkerhet behöver införas mer distribuerat och mer på ändpunkterna än tidigare säkerhetsfokus som främst legat på skalskydd. En tydligt fokus behöver också läggas på användarens säkerhet som trots allt fortsätter att utgöra den största attackvektorn i IT-miljön.

Om författaren

Björn Videnberg är lösningsarkitekt på Conscia. Han var CCIE 2001-2012 och har över 20 års erfarenhet av IT-branschen varav 15 år med kvalificerade lösnings- och säkerhetsprojekt på bland annat IBM. Hans expertområden inkluderar säkerhet, nätverk, och datacenter. Ett särskilt expertområde är just praktisk erfarenhet kring hur säkerhet skall införas i komplexa miljöer.

Om Conscia Sverige

Systemintegratören Conscia Sverige erbjuder kvalificerade lösningar och konsulttjänster med spetskompetens inom Datakommunikation, IT-säkerhet, Datacenter och Operatörsnät. Vår egenutvecklade programvara CNS säkerställer tillgänglighet, prestanda och Compliance för våra kunder. Vi är Guldpartner till Cisco, Cisco Customer Experience Partner of the Year och fokuserar våra lösningar på Ciscos teknologi. Conscia Sverige är en del av den europeiska Conscia-koncernen med över 500 anställda i Sverige, Danmark Norge, Nederländerna, Slovenien och Tyskland. www.conscia.com/se