TEMA:

"DEN MODERNA DISTRIBUTÖREN"

- "Nya kapitel, nytt kapital"!
- ”Många faror lurar på våra endpoints!”
- ”Om du inte kan se, har du inte koll!”
- ”Ynkligheten når nya nivåer!”
- ”Det är säkrast att tänka efter före”

EXCLUSIVE NETWORKS

Exclusive Networks
– Nya kapitel, nytt kapital!

Exclusive Networks fortsätter sin imponerande tillväxtresa!
Nya tjänster breddar deras service-utbud och etablering i fler länder leder till fortsatt globalisering.
Lägg därtill en nyligen genomförd börsintroduktion.

Det är svårt att inte bli imponerad av den utveckling som Exclusive Networks visar upp år efter år. I september 2021 börs-introducerades de på Euronext (European New Exchange Technology) i Paris. Det ger oss muskler att fortsätta vår globala expansion", säger Patrik Tamker som är Country Manager för Exclusive Networks Sverige och Nordic Director.
En distributör med ett genomtänkt erbjudande. Han beskriver företaget som en global distributör som drivs av Cyber Security och Cloud Services.

"När vi startade för 12 år sedan var vi 80 medarbetare i 8 länder. Nu är vi cirka 2000+ anställda och vi finns i mer än 40 länder från Australien/Nya Zeeland till Asien, Europa, Afrika och vidare till Nordamerika. Sydafrika är det senaste tillskottet och där startade vi upp i slutet av 2021", berättar Patrik stolt.

Han menar att alla marknader har sina förutsättningar respektive affärskulturer och därför är den lokala närvaron mycket viktig. En annan tydlig pusselbit i deras framgång är att de arbetar aktivt med att hjälpa deras partners och leverantörer att få chansen att bygga sina varumärken. Bland annat med event men också genom att erbjuda utbildning baserat på många av de leverantörer Exclusive Networks representerar. Här finner vi ännu ett exempel på Exclusive Networks ständiga utveckling. En ny plattform för Global Training har precis lanserats.

Andreas Lindén, Försäljningschef, lyfter fram en annan sak: ”Vårt partnerupplägg gör att vi kan hjälpa alla kunder”.

Det ena ger det andra.
En intressant iakttagelse är Exclusive Networks tjänstekatalog. Efterhand som de har växt har de skaffat sig insikter inom nya områden. Den kunskapen har de sedan paketerat för att komplettera sitt erbjudande.

Ett exempel på det är deras Deployment Services där deras erfarenheter av globala utrullningar har lett till ett intressant erbjudande av konsult- och tekniktjänster inom import/export-relaterade områden. RMA (Return Merchandise Authorization) är ett område som växer fort bland annat på grund av ökat miljöfokus. Det handlar om hantering av den utrustning som blir överflödig till exempel vid en uppgradering eller ett byte av teknisk plattform. Exclusive Networks har både erfarenhet och kunskap om RMA och kan hjälpa till med att få hem utrustning som sedan hanteras på en eftermarknad eller destruktion.

Nya konsumtionsmönster ändrar marknaden

Ett annat område där de lanserar nya lösningar är inom konsumtion där de stora molnaktörerna ändrar marknaden som går mer och mer mot ett ”As A Service”-tänk. Här vill de fylla det kunskapsgap som de ser. Därför har de byggt en plattform, X-OD (Exclusive On Demand), för konsumtion av teknik. I Norden kommer den att lanseras senare i år. Den är prenumerationsbaserad vilket gör att kunderna inte behöver ha ett finansbolag inkopplat.
Om en klassisk finansiering skulle behövas i något annat sammanhang så har de även det i sitt breda erbjudande. Det ska bli spännande att se vad som blir nästa kapitel i berättelsen om Exclusive Networks.

EXCLUSIVE NETWORKS

”Många faror lurar på våra endpoints!”

På grund av alla cyberattacker gäller det att vara på sin vakt. Behovet av ökad säkerhet växer kontinuerligt med tanke på att vår perimeter, där skydd behövs, flyttas

En kapprustning, inom säkerhet, pågår sedan länge mellan cyberkriminalitet och IT-säkerhet. Vid fronten finns våra endpoints i form av smarta mobiler, surfplattor, bärbara datorer och inte minst alla saker som är uppkopplade i våra hem. De är alla måltavlor för de cyberkriminella.

Det började med Antivirus

Det som en gång började med att vi skulle skydda oss genom att installera ett antivirus har under åren utvecklats till alltmer avancerade lösningar i takt med att hotbilden har ändrats. Faktum är att nya säkerhetsrisker inte bara skapas av hackarna. Vår egen önskan om att det ska vara enkelt att koppla upp sig samt att vi vill kunna göra det var vi än befinner oss gör oss användare till de största attackytorna. Att till exempel Phishing-mail inte har försvunnit är ett tydligt tecken på att hackarna fortfarande tjänar pengar på de utskicken. Den pågående pandemin har skapat nya förutsättningar eftersom antalet som distansarbetar har ökat lavinartat. Även om vi nu förhoppningsvis ser slutet på pandemin så är det många som inte tror att omfattningen av distansarbete kommer att återgå till tidigare nivåer. Exclusive Networks tillhandahåller, via sina partners, flera olika lösningar när det gäller cybersäkerhet. Ett effektivt verktyg är EDR (Endpoint Detection & Response). Vi träffar Ola Andersson och Marcus Fredlund som båda är Sales Engineer på Exclusive Networks. De har full koll på EDR och varför det har blivit en viktig del av ett totalförsvar i kampen mot bland annat dataintrång och Ransomware-attacker.

Analysen är styrkan i EDR

”Hur trist det än är att behöva säga det här, så är det bara att konstatera att det finns ingen IT-säkerhetslösning som är 100 % säker! Traditionella antivirusprogram bevakar att ett intrång inte sker utifrån de hot som redan är kända. Det är givetvis en bra början men hur hanterar du hot som du inte känner till?”, säger Ola inledningsvis.

”Det är här som styrkan i EDR kommer in i bilden. Det handlar om kraftfulla analyser, baserade på AI (Artificiell Intelligens) och ML (Maskininlärning). De tittar på vad som pågår i de uppkopplade endpoints vid varje givet tillfälle. Så fort kända mönster bryts eller trafiken plötsligt ökar markant kan det indikera att ett intrång är påbörjat. Eller om en enhet som förväntas finnas i Sverige helt plötsligt dyker upp i ett annat land och vill få tillgång till det som den i normala fall brukar anropa”, fortsätter Marcus. Förutom analysen lyfter både Marcus och Ola fram inspelningsfunktionen som en mycket viktigt del i EDR. Den möjliggör att man i efterhand, i detalj, kan se vad som skett och även gå tillbaka i tiden för att jämföra med hur trafiken såg ut vid olika tillfällen.

De berättar att ytterligare en fördel med EDR är att trafiken i endpoints inte är krypterad vilket gör det enklare att se vad som pågår. De upplever också att fokus på att skydda endpoints har ökat markant vilket sannolikt beror på våra ändrade arbetssätt.

Mitt hem är min borg!

Vi avslutar vårt samtal med att konstatera att förutom att den mänskliga faktorn är den största säkerhetsrisken är det sannolikt att våra hem ligger tvåa på den oglamorösa listan. Marcus och Ola menar att de uppkopplade sakerna i våra hem oftast inte är patchade med de senaste uppdateringarna och att det sannolikt är väldigt ovanligt att hemmanätet är segmenterat så att de enheterna är uppkopplade separat i hemmet. Det finns exempel på Youtube där man kan se en robotdammsugare som åker runt i ett hem och filmar (!) samtidigt som den ritar upp en karta över hemmet.

Med tanke på alla digitala fällor, som finns runt omkring oss, känns det bra att det finns personer som Marcus Fredlund och Ola Andersson på Exclusive Networks. De har full koll på alla aspekter avseende IT-säkerhet.

”Om du inte kan se, har du inte koll!”

Det finns många tjänster och verktyg inom IT-säkerhet. En sak som utmärker de allra bästa lösningarna är genomtänkt visibilitet. För att kunna göra de rätta analyserna måste det tydligt synas vad som pågår.

Det kan tyckas som den självklaraste sak i världen att man måste kunna se vad som händer i sin IT-miljö för att sätta in rätt åtgärd. I takt med att lösningarna för att upptäcka och stoppa dataintrång har blivit kraftfullare, levererar de mer och mer information. Det gamla ordspråket – Man ser inte skogen för alla träden – gör sig påmint. Mängden information kan helt enkelt bli så omfattande att det blir svårt, eller omöjligt, att faktiskt tolka vad det är som händer i det egna nätverket.

Som att titta rakt in i solen

Ola Andersson och Marcus Fredlund, som båda är Sales Engineer på Exclusive Networks, förklarar varför visibilitet är en mycket viktig del av en modern säkerhetslösning. ”När vi är ute och pratar om våra lösningar, inom bland annat EDR och NDR, lyfter vi alltid fram vikten av en bra och genomtänkt visibilitet. Ibland kan det nästan kännas lite fånigt att prata om det eftersom det är så självklart att det är bra att man kan se vad som händer eller har hänt. Vår poäng är inte bara att man kan se nätverkstrafiken utan det viktiga är hur informationen presenteras”, förklarar Ola.

”Idag är det möjligt att få ut analyser och rapporter med i princip hur mycket information som helst. Desto mer information, desto större risk att de viktigaste signalerna försvinner i mängden. Vi vill vara tydliga med att vi nu pratar om analyser och rapporter som ska granskas av ett mänskligt öga”, fortsätter Marcus.

”I den löpande maskinella övervakningen blir automation vanligare. Allt oftare att det är AI- och ML-lösningar som håller koll.

Det är när något upptäcks som det blir extra viktigt att visibiliteten är genomtänkt. Annars blir det som att titta rakt in i solen. Du blir blind", fyller Ola i.

Flera dåliga beteenden ger rött kort

En av flera saker som övervakas är hur olika användare och enheter beter sig. Det handlar mycket om att analysera beteenden som till exempel vilken data man vill komma åt. Om någon gör flera konstiga saker kan den användaren stoppas automatiskt och sättas i karantän i nätverket.

En annan sak som Ola & Marcus lyfter fram är behovet av att kunna se var ditt data befinner sig och vem som hanterar det, så kallad datavisibilitet. Därför finns det en annan mycket viktig funktion. Det är möjligheten att kunna spela in vad som händer i ett nätverk och uppkopplade enheter. Det gör att man kan hitta tidpunkten för när ett dåligt beteende uppträdde för första gången. Om man behöver använda en backup för att återställa sin IT-miljö är det en ovärderlig information att veta hur långt tillbaka man behöver gå när det gäller att bestämma vilken backup som ska användas.

Tillsammans blir vi starkare!

Marcus och Ola berättar att det finns ett intressant samarbete mellan olika aktörer inom IT-säkerhet. Syftet är att hjälpa varandra att upptäcka intrångsförsök och nya hotbilder. Det innebär i praktiken att olika system håller varandra informerade när nya dåliga beteenden upptäcks.

"Alla tjänar på det här utbytet av information. Jag tycker att det är ett sundhetstecken att branschens aktörer, även om de är konkurrenter, samarbetar för att bemöta den gemensamma fienden; cyberkriminaliteten", säger Marcus.

"En kundgrupp som får extra fördelar är de mindre företagen som kanske inte har möjlighet att investera i de största och dyraste lösningarna. Det här gör att även de mindre leverantörernas lösningar får ta del av den information som de stora aktörerna delar med sig av", förklarar Ola.

Mötet med Marcus Fredlund och Ola Andersson påminner oss om den breda och djupa kompetens som Exclusive Networks har byggt upp tillsammans med sina partners och leverantörer. Det skapar en trygghet för deras kunder.

”Ynkligheten når nya nivåer!”

Ransomware är ett att av de vanligaste hoten inom dagens IT-säkerhet enligt flera rapporter, där ibland Splunks ”Top 50 Security Threats”. En av flera saker som kännetecknar Ransomeware är den extrema kallsinnigheten när det gäller valet av måltavla.

I korthet betyder Ransomware att någon tar kontrollen över läsbarheten av sparad data i någon annans IT-miljö. För att ge tillbaka kontrollen kräver angriparen att offret betalar en lösensumma (engelskans Ransom) för att återfå tillgången till sitt data. Det är med andra ord en digital variant av en klassisk kidnappning.
De svagaste eller naivaste är ofta offren
Alla former av cyberkriminalitet är givetvis förkastligt men frågan är om inte Ransomeware är en av de smutsiga varianterna. Anledningen är att de cyberkriminella ofta väljer verksamheterna och marknader som är extra sårbara, till exempel hälso- och sjukvården.

Många har fullt upp med att överhuvudtaget hålla i gång sin verksamhet och fokus på att hålla sina IT-system uppdaterade med de senaste uppdateringarna ofta kommer i andra hand. Hackarna bryr sig inte ett dugg om det, snarare tvärtom. De väljer helt känslokallt att sikta in sig på de verksamheter som redan går på knäna eller inte har insett vikten av att hålla sina IT-system uppdaterade.
En aktör som tar upp kampen mot Ransomware är Exclusive Networks. Vi frågar deras sakkunniga Magnus Pettersson, Sales Engineer – Cloud Solutions, och Ola Andersson, Sales Engineer, om vad som är viktigt att tänka på för att undvika att bli drabbad av en Ransomeware-attack.
”En av de absolut viktigaste sakerna är att ha koll på sin plattform för backuper. Många Ransomeware-attacker börjar med att försöka slå ut de backuper som finns i den IT-miljö som attackeras.

Allt för att skapa så stor skada som möjligt. Därför är det helt vitalt att ha en fungerande ”Restore-funktionalitet”. En annan viktig del är att ha en uppbyggd kunskap bland medarbetarna om att identifiera Phishing-mail. De utgör en stor del av den totala hotbilden när det gäller Ransomeware-attacker”, säger Ola.
”Ransomware har funnits ett bra tag och det kommer fortsätta att finnas kvar så länge som cyberkriminella ser att det finns pengar att tjäna på det. Det är den bistra sanningen”, fyller Magnus i.
Ingen källarverksamhet
Oavsett om Ransomeware började som någon form av digitalt pojkstreck eller inte så står det helt klart att det i dag har utvecklats till en professionell verksamhet som kan jämställas med ett helt vanligt företag. Offren behandlas som deras kunder. En del av upplägget är att göra det attraktivt för ”kunderna” att enkelt kunna göra sina betalningar genom tydliga och pedagogiska instruktioner.
Alla de som bekämpar denna form av kriminalitet har ett entydigt budskap – Betala inte lösensumman. Därför vill hackarna att det ska vara enkelt att ändå betala för att få tillbaka sitt data. Oavsett vilket val den drabbade organisationen väljer måste de fundera på vilket data som de har förlorat kontrollen över.

Det här är väldigt svårt att veta. Sannolikt är det så att de flesta företag inte har full koll på vad som saknas på deras kontor om de skulle drabbas av ett vanligt fysiskt inbrott.

”Därför är det så oerhört viktigt att du har full koll på ditt data samt viken information det är som saknas eller har kopierats efter en Ransomeware-attack. Nästa fråga, om du väljer att betala, är hur vet jag att jag har fått tillbaka all data?”, förklarar Ola.

”Vid en Ransomeware-attack är det vanligt att man först förstör backuperna. Därefter börjar man kryptera data så att det inte blir läsbart. Krypteringen sprids ut över den totala datamängden för att skapa största möjliga skada på kortast möjliga tid. Dessutom sker attackerna ofta på helger för att få tillgång till så mycket CPU (datorkraft) som möjligt samt att det ska dröja innan attacken upptäcks”, säger Magnus.
Finns det då ingen positiv faktor inom denna hotbild?
Jo, Magnus och Ola berättar att tiden från att en Ransomeware-attack inleds till att den upptäcks ständigt minskar. Med moderna skyddsverktyg kan man snabbt stoppa den användare som intrånget styrs ifrån.

”Det är säkrast att tänka efter före”

För några år sedan dök det upp ett nytt kraftfullt verktyg i verktygslådan för IT-säkerhet, nämligen Network Detection and Response. Vi kontaktade Exclusive Networks för att få veta mer.

Nicklas Helleday, Inside Sales, och Joakim Strömgren, Sales Engineer, på Exclusive Networks har full koll på Network Detection and Respons (NDR) och dessutom IT-säkerhet i stort. Vi bokar ett möte med dem för att få veta mer. De delar gärna med sig av sin kunskap.

”Faktum är att en stor utmaning för oss är att alltför många företag och organisationer inte har ett specifikt säkerhetstänk. De tycker att IT-säkerhet är ett nödvändigt ont. Det finns alldeles för få som verkligen kan IT-säkerhet”, inleder Joakim.

”Bara Ransomware omsätter någonstans mellan 200 och 500 miljoner dollar per år 1. Det är givetvis en uppskattning eftersom långt ifrån alla lösensummor som betalas blir kända”, fortsätter Nicklas.

En billig och alltför ofta missad åtgärd
De berättar för oss om en intressant detalj som, rätt hanterad, skulle kunna höja väldigt många företags IT-säkerhet. Dessutom är det en billig åtgärd som snabbt skapar ett bättre skydd mot intrång. Vi talar om hanteringen av lösenord.

Om du tar en vanlig hyggligt kraftfull gamingdator och programmerar om grafikkortet för att knäcka lösenord så tar det inte lång tid innan du har lyckats, generellt sett. Dessutom har de cyberkriminella gott om tid så även om det tar någon dag så är det inget problem för hackarna”, säger Joakim.

Vi får en tydlig bild av hur viktigt det är med starka lösenord när vi får veta hur lång tid, ungefär, som det tar att knäcka lösenord med olika svårighetsgrad. Se faktarutan här intill.

”Det borde vara ett krav från företagen att deras anställda använder starka lösenord. Det gör man enklast genom att IT-systemen inte accepterar svaga lösenord. Ett annat problem är att väldigt många använder samma lösenord på flera, kanske alla, ställen. Där handlar det om att göra användarna medvetna om riskerna och få ett bättre säkerhetstänk inom företaget”, menar Joakim.

APT-grupper är ett av många hot
De cyberkriminella blir mer och mer organiserade.

Det finns till exempel cirka 400 APT-grupper (Advanced persistent threat) runt om i världen 2. De arbetar uteslutande med att komma åt data som de antingen kan ”kidnappa” och begära en lösensumma för att lämna tillbaka kontrollen över = Ransomware. Det kan också handla om att datat i sig är värdefull information som kan säljas till intresserade köpare. De ”vanliga” hackarna är oftast lata och söker hela tiden efter den enklaste vägen in. Det kan vara ett installerat fläktsystem som är uppkopplat och har en IP-adress. ”Tyvärr är det väldigt vanligt att man inte ändrar standardlösenordet i samband med installeringen av olika typer av utrustningar och maskiner. Du kan enkelt googla efter vilket lösenord som gäller för en maskin från en specifik leverantör”, förklarar Joakim.

Du ska vara jobbigare än dina konkurrenter. Hur ska ett företag tänka för att skydda sig mot intrång?

”Det finns en del relativt enkla åtgärder som man kan börja med. Att kräva att användarna har starka lösenord har vi redan nämnt men det är viktigt. Att utbilda sin personal med målet att alla ska ha ett gemensamt säkerhetstänk är också viktigt. 95 % av alla attacker är så kallad Phishing där man, ofta via e-post, försöker lura till sig inloggningsuppgifter 3.

Därför är det viktigt att de anställda är utbildade och vaksamma. Det kan även vara klokt att klassificera alla anställda och skapa olika grupper som kommer åt olika delar av IT-miljön. Alla behöver oftast inte komma åt allt”, säger Nicklas. Mobiltelefonerna utgör en annan risk. Även när vi inte använder mobilen så ”pratar” den hela tiden med andra mobiler. Vi rekommenderar starkt att man använder dubbel autentisering för sina smarta telefoner”, berättar Joakim.

”Vi brukar säga att man ska vara jobbigare än sina konkurrenter. Om en hackare ska välja mellan två likvärdiga mål är det företaget med sämst skydd som drabbas av ett intrång”, säger Nicklas.

”NDR gör dig ”jobbig” att hacka!
Ett sätt att ”vara jobbigare” är att investera i en NDR-lösning, Network Detection and Respons. Det är svårare att stjäla en bil som är i rörelse än en som är parkerad. Det är samma sak med data. NDR tittar på allt som skickas respektive händer i ett nätverk. Så fort ett avvikande mönster uppstår sker en kontroll av det. Dessutom spelas allt in vilket gör att man i efterhand kan gå tillbaka och se vad som hände. En tidslinje som kopplas till inspelningen gör det enklare att följa upp när och var något skedde. NDR bygger bland annat på maskininlärning (ML) och ger en effektiv övervakning av IT-miljön, utifrån och in. Nicklas och Joakim gör en liknelse med en dörrvakt på en krog. Vaktens uppgift är att inte släppa in stökiga och otrevliga gäster.

Vad händer om en till synes trevlig och lugn gäst passerar vakten men senare på kvällen, efter några timmar i baren, startar ett bråk inne på krogen? En NDR-lösning håller koll på hela ”krogen” dygnet runt.
NDR är på väg att bli en självklarhet
NDR har funnits i 3-4 år och är på väg att bli en lika naturlig del av en IT-säkerhetslösning som brandväggen en gång blev, i IT-säkerhetens barndom.

”Vår upplevelse är att alla vill ha NDR och att det är nu som NDR på allvar gör entré inom IT-säkerhet”, förklarar Joakim.

”NDR kompletterar SOC (Security Operations Center) och EDR (Endpoint Detection and Response) på ett utmärkt sätt. Gartner lyfter också NDR som en viktig del av en totallösning inom IT-säkerhet”, avslutar Nicklas.

Efter vårt möte konstaterar vi att det finns tillfällen när det är bra att vara ”jobbig”!

Exclusive Networks är en global cybersäkerhetsspecialist för digital infrastruktur som hjälper till att driva övergången till en fullständigt pålitlig digital framtid för alla människor och organisationer.
Vårt distinkta synsätt på distribution ger partners fler möjligheter och tydligare kundrelevans. Vår specialitet är deras styrka – att utrusta dem för att dra nytta av nya innovativa teknologier och transformativa affärsmodeller. globala med en ”services 1st ideology”, som använder innovation för att leverera partnervärde.
Med kontor i 43 länder och förmågan att betjäna kunder i över 170 länder på fem kontinenter, har Exclusive Networks en unik modell för "lokal försäljning i global skala", som kombinerar värdet av en lokal oberoende tjänsteleverans med en global distributionskraft.

Låt Exclusive Networks vara din startpunkt – vi hjälper dig!
exclusive-networks.com/se
Mail info@excluisve-networks.com

EXCLUSIVE NETWORKS