Säkerhet Utökad Skydd

Slutrapport – utkast

Sammanfattning

Det här projektet har haft som målsättning att undersöka ämnesområdet Next-Generation firewall, under rubriken Säkerhet Utökat Skydd, för att se hur dessa skulle kunna passa in på lärosätet, och vilka fördelar man kan se om ett lärosäte väljer att implementera en sådan lösning.

Rapporten är indelad i fyra delar, introduktion, policy & roller, arkitektur samt ett appendix innehållande ett urval av leverantörers kommentarer på rapporten.

Avgränsningar

Vi har i projektet enbart behandlat vad man brukar kalla en "appliance", alltså en fysisk hårdvaruenhet som innehåller de funktioner man normalt tillskriver en next-generation firewall, något som även kallas enterprise firewall.

Det innebär att vi i inte har övervägt andra metoder att åstadkomma samma funktionalitet med andra mer funktionsspecifika verktyg, utan vi har enbart behandlat en mer eller mindre färdig paketlösning som går att beställa.

Policy & Roller

Policy och riktlinjer

För att undvika att policys och riktlinjer måste uppdateras ofta så ser vi att man håller den väldigt generell. Det gör att man snabbare kan anpassa sig till nya och förändrade hotbilder utan att behöva ett rektorsbeslut.

När det gäller vilka typer av websidor och liknande som är tillåtet att ansluta till så ser vi att man hänvisar till de befintliga policys som gäller etik och moral. Det är inte IT-avd ansvar att bestämma detta. Vi ser också att man kan hänvisa till SUNET:s regler istället för att skriva med de ordagrant. Detta för att inte behöva uppdatera policyn om SUNET ändrar sina regler.

Det finns också en risk för att man förbjuder för personal som forskar att fullfölja sitt arbete utan att bryta mot dessa regler då.

Det man kan göra är att ta fram en process för undantag när man har personal som ska komma åt den typen av material.

Regelverket bör också vara kopplat till vad man får göra som person och inte vad man får göra från en viss typ av enhet. Det är vad man gör som är det viktiga inte vilken typ av enhet man använder. Det här gör också att man inte behöver uppdatera policys när det kommer nya typer av enheter som används.

Det är också viktigt att ta med information om vad som händer om man bryter mot reglerna. Det kan t.ex. vara avstängning från nätverket men också att personen i ifråga blir polisanmäld.

För att kunna upptäcka eventuella brott mot policys och riktlinjer samt upptäcka hot och skadlig kod så måste man kunna övervaka användandet både av enheter och nätverkstrafik. Det är viktigt att man får information om det så att alla är medvetna om att övervakning sker och loggas.

Eventuellt kan det vara nödvändigt att även titta på krypterad trafik för att få en helhetsbild om den trafik som går på nätverket. Här behöver man göra en avvägning om vad och hur mycket som man kan göra utan att göra alltför stort ingrepp på den personliga integriteten eftersom man då kommer att ha möjlighet att komma åt känslig information.

Roller

För att kunna införa och hantera drift och larmhantering från NGFW och IPS krävs att man har personal med rätt kompetens. Det här är blir svårt för de lärosäten som har små IT-avdelningar eftersom man inte har tillräckligt med personal som har rätt kompetens. Samtidigt så är det så att

ett NGFW-verktyg kommer att ge bättre överblick på vad som faktiskt händer på nätet, minder antal incidenter att ta hand om och frigöra tid då saker kan stoppas i förtid.

Ansvaret för den här typen av lösningar ska ligga antingen hos ett dedikerat team som jobbar med säkerhetsfrågor eller hos de som driftar nätverket. Det är viktigt att rutiner eller policys tas fram för hur regelinställningar och förändringar utförs, dokumenteras och var dokumentationen sparas för att säkerställa ett konsekvent och kontinuerligt arbete.

För hantering av larm så kan personalen som hanterar dessa även ha andra roller. Det blir då lättare att få tillräckligt många personer med kompetensen för att klara semestrar, sjukdom osv. Man kommer också bort från problemet med personberoenden. Det behöver finnas möjlighet att delegera olika roller som t.ex. enbart läsning för vissa segment.

På sikt så bör ambitionen vara att automatisera hanteringen av larm och att endast larm som är kritiska hanteras manuellt.

En viktig aspekt i det hela är att det är ett väldigt känsligt system där det finns känsliga personuppgifter i. Det gör att det endast är utpekad personal som ska ha tillgång till det. Speciellt om man väljer att titta på krypterad trafik.

Eftersom så mycket som möjligt ska ske automatiskt i ett NGFW kommer användarna av systemet att bli utestängda från nätet när så behövs. Det är viktigt att en tydlig kommunikationspunkt finns mellan användarna och IT. Det naturliga är att användarna kan vända sig till ServiceDesk för en första information om vad som har hänt och därifrån hänvisas för lämpliga åtgärder.

Hotbild

Eftersom hotbilden kan ändra sig fort så är det viktigt att de policys och riktlinjer man har stödjer detta, dvs är generellt skrivna. Om policys och riktlinjer måste revideras när det kommer nya hot så kommer man inte att kunna implementera de nödvändiga skydd som behövs. Idag ser universitetsvärlden omfattande hot i form av industri-, ekonomiskt- samt flyktingspionage.

Mekanismer man använder sig för intrång idag är ofta:

- Exploit kits.
- Personer som försöker hacka system, både internt och extern.
- Personer som försöker hacka andra företag/organisationer från de interna näten.
- Portskanningar
- Phishing
- Ransomware
- Bitcoin m.m.

Då våra automatiska system blir allt bättre och mer förfinade kommer vi att utsättas för olika typer av attacker genom social engineering. Vi ser redan nu attacker via mail som är mer eller mindre välgjorda. I framtiden kommer vi att se ännu mer av denna typen av attacker som antingen övergår till mobiltelefon eller där förövarna börjar kombinera ett eller flera kontaktmedier för att ta sig förbi

våra automatiska digitala system. Även insider-brott kommer att komma, då vi skyddar oss så väl utåt men inte alltid har den bästa säkerheten bakom brandväggarna.

Mail i sig är ett osäkert sätt att kommunicera på som inbjuder till olika former av attack-vektorer, men vi tror inte att mail kommer att försvinna inom den närmaste framtiden.

Säkerheten i molntjänster får inte glömmas bort. Vi måste se till att dessa är lika skyddade som om de satt på campus. I många fall är inloggningen till en molntjänst en epost-adress vilket gör dessa tjänster enkla att utsätta för attacker. Hackarna kartlägger vår verksamhet noga och kan ta reda på vilka som kan vara aktuella för en attack.

För att minska belastningen på den befintliga tekniska personalen så är vill vi att så mycket larmhantering som möjligt automatiseras. Endast de larm som inte tas om hand automatiskt ska gå till teknisk personal för analys.

Sedan måste det vara möjligt att få ut statistik ur systemen för uppföljning och rapportering.

Arkitektur

När man angriper den faktiska arkitekturen man vill implementera är det viktigt att man tänker sig ett successivt införande. Det är inte säkert, det är förmodligen högst otroligt, att man kan nå målet utan att ha gått igenom ett införande som får ta tid och gå försiktigt fram. Vid en större förändring av en så grundläggande infrastruktur där man riskerar att utesluta delar av verksamheten är det viktigt med inkrementella förändringar och kontinuerlig återkoppling, för att kunna fånga upp alla randvillkor man kanske inte hade med från böran. Man kanske till och med lyckas belysa delar av verksamheten som fram tills nu var helt okända. Här är det viktigt att man väljer en arkitektur som ger så många möjligheter som möjligt att planera införandet, samtidigt som man inte skall hamna i en rävsax längre fram som stänger möjligheten att för vissa delar av verksamheten att fortsätta sitt arbete ohindrat.

Redundans

För att åstadkomma redundans brukar en next-generation firewall lösning oftast konfigureras som ett kluster av två. Dessa kan konfigureras antingen som active/active eller active/standby, vilka har olika för och nackdelar. Active/active innebär att båda hårdvaruenheter arbetar tillsammans och upprätthåller gemensam syn på sin tillvara genom att synkronisera det övergripande tillståndet emellan sig. Active/Standby innebär att en enhet arbetar medan den andra är helt utan last och enbart får tillståndet synkroniserat från den aktiva enheten. Om den aktiva enheten slutar fungera eller på något sätt triggar en s.k. "failover" så tar den passiva enheten över.

Det är viktigt att man tidigt säkerställer om den lösning man planerar att införa tillåter asymmetriska trafikflöden, samt vilka eventuella begränsningar som kan finnas i just den lösningen man valt. Det kan exempelvis bli omöjligt att längre fram styra trafiken som man planerat om det finns en begränsning man inte informerats om.

Begränsningar man skall tydligt undersöka är om man har ett kluster konfigurerat Active/Active är det isåfall möjligt att trafiken i olika riktningar passerar den andra klustermedlemmen. Det är inte självklart att detta är möjligt och det kan variera mellan leverantörer.

Möjlig placering

Vid en inkoppling av en appliance i lärosätets nätverk finns det ett par vanliga scenarier. Normalt har man sett en brandvägg som en skiljelinje mellan fysiska nätverkssegment, kanske genom att helt enkelt placera en brandvägg där lärosätets nät möter Internet. Tidigare har man ofta betraktat oönskad trafik kommande utifrån, men i dagsläget är hoten olika och beter sig på olika sätt. Oönskad trafik kan lika gärna komma inifrån.

Det finns många olika metoder att använda sig av när man tänker på var man vill placera sin appliance. Det är möjligt att placera en appliance mellan två routrar exempelvis, och låta den vara till största delen transparent men med möjlighet att direkt blockera oönskad trafik. Det är här även möjligt att spegla trafik från utvalda portar, eller dela på ljuset i en fiber, och på detta viset få

möjligheten att enbart observera trafiken. I det senare exemplet behöver man använda en annan metod att blockera trafik, saknar man den möjligheten idag är det inte en metod vi rekommenderar.

Grundläggande nätverkssegmentering

Innan man planerar sin appliance är det viktigt att man försöker inventera sitt nätverk så att man har en kristallklar bild över vilka nätverkssegment man har, vilka som behöver skydd och vilka som inte behöver skydd. Olika lärosäten kan ha valt olika sätt att segmentera sina nät, vissa kanske har kommit undan utan att göra det överhuvudtaget. I det senare fallet är införandet ett bra tillfälle att segmentera upp sitt nät. Det kanske finns skäl att förändra segmenteringen, då det som finns idag kanske inte längre är relevant och baserades på en struktur som genomgått flera omorganisationer sedan dess.

En någorlunda självklar distinktion är server och klient. Man har oftast ett servernät någonstans där servrar snurrar, klientnät kanske är mer diffusa och det finns säkerligen klientnät som även innehåller en del servrar. Det finns kanske en del labnät, studentnät osv. Det viktiga är att man har en klar bild över hur var de finns och hur access sker idag. Ett införande hänger på att man väljer vilka segment man vill lyfta in i lösningen man valt.

Placering i Core

Vi har dragit slutsatsen att ett smidigt införande sker om man placerar sin lösning direkt ansluten till sitt core, och använder sig av routing för att styra trafik mellan nätverkssegment genom appliancen. Trafiken kan styras genom att man sätter up VRF instanser (virtual routing and forwarding). VRF gör det möjligt att logiskt se sitt core som flera olika, med olika skyddsgrad.

Den stora vinsten med att utföra införandet genom VRF instanser är att man kan göra det successivt och man kan enkelt välja att backa ur om det inte fungerade som man tänkt.

Tekniska Krav

Full routing

En next-generation firewall behöver minst stödja full routing och routingprotokoll för både ipv4 och ipv6 som används ute i lärosätena för att den skall kunna samexistera med den övriga infrastrukturen.

Länkaggregering

Länkaggregering (LACP) måste stödjas fullt ut.

API

Det skall finnas ett API tillgängligt som är lätt integrerbart med eventuella verktyg man använder ute i verksamheten. API:t bör använda sig av vanliga metoder för API-åtkomst och skall ha exempel på integrering med marknadsledande konfigurationshanteringsverktyg (puppet, chef ansible etc.)

Larm

Larm skall kunna exporteras till andra system. Helst genom ett öppet väldokumenterat maskinläsbart format som exvis json. Enheten måste även stödja syslog.

Kunna använda "bespoke" användar-id källor

Det skall gå att använda sig av helt egenutvecklade källor för vem som använder en viss enhet. Det finns ofta metoder för att ansluta ett system till active directory, det skall vara möjligt att använda sig av ett API för att ge samma information till systemet från exempelvis en radius-server eller liknande.