Jobbar ni tillräckligt proaktivt med IT-säkerhet?

INNEHÅLL

Introduktion	3
Om Axians	4
MSB rekommendationer	5
Installera säkerhetsuppdateringar så fort det går	5
Förvalta behörigheter och använd starka autentiserings-funktioner samt begränsa och skydda behörigheter	6
Inaktivera oanvända tjänster och protokoll	9
Säkerhetskopiera	10
Tillåt endast godkänd utrustning i nätverket	11
Säkerställ att godkänd mjukvara används	13
Uppgradera mjuk- och hårdvara	14
Säkerställ förmåga att upptäcka säkerhetshändelser	15
Segmentera nätverken	18
Slutord	19

INTRODUKTION

Som alla är högst medvetna om är vi påverkade av det säkerhetspolitiska läget som pågår runt oss. Sverige har på olika sätt en förhöjd hotbild, inte minst när det gäller cyberattacker. Det skapar oro och för många kan det vara svårt att veta vad man ska göra.

Som IT-leverantör och driftpartner för komplexa IT-miljöer där Axians kunder inte sällan spelar en samhällsviktig roll, har Axians ett stort ansvar för att garantera maximal tillgänglighet och hög säkerhet.

MSB, Myndigheten för Samhällskydd och Beredskap, trycker på hur viktigt det är att alla typer av organisationer och verksamheter ser över sina IT-miljöer och har publicerat ett antal rekommendationer som talar om för alla som ansvarar för IT-system, vad som behöver göras för att passera en godkänd nivå.

För att ni ska få en tydlig och enkel överblick av MSBs grundläggande rekommendationer för vad som krävs för att säkra upp IT-miljön, har vi därför sammanställt dem i detta white paper.

Under varje rekommendation kan ni också läsa om Axians lösningar och Axians tjänster som gör att rekommendationerna hanteras på ett professionellt sätt.

OM AXIANS

Som våra kunders IT-partner är vårt uppdrag att säkra våra kunders informations-tillgångar och leverera förstklassig vägledning och expertis i nära dialog och med öppenhet. Vi ligger alltid ett steg före genom preventiv vägledning och är en IT-partner som du kan räkna med. Dygnet runt och året runt. Våra expertisområden är följande: Cloud & Datacenter, Cybersecurity, Enterprise networks, Professional Services, ServiceNow och Digital workplace.

Vi är en global partner med lokal närvaro. Axians AB har 160 anställda och Axians globalt har 12 500 anställda i 27 länder. Det svenska huvudkontoret ligger i Stockholm.

MSB REKOMMENDATIONER

Nedan följer MSBs rekommendationer följt av information om hur Axians lösningar kan hantera den rekommenderade åtgärden:

INSTALLERA SÄKERHETSUPPDATERINGAR SÅ FORT DET GÅR

MSB säger: För att minska den vanligt förekommande risken att en angripare utnyttjar kända sårbarheter i hård-och mjukvara är det viktigt att installera säkerhetsuppdateringar så snart det är möjligt.

Axians lösning: ”OS Management” är Axians tjänst för drift och underhåll av server-operativsystem. Tjänsten är avsedd för företag och organisationer som behöver tillgång till en servermiljö med förstklassig prestanda, stabil drift och hög tillgänglighet.

Servern kan antingen ägas av kunden eller vara en server i Axians skyddade och säkrade eller vara en server i Axians skyddade och säkrade datacenter.

Kunder som köper ”OS Management” får en servermiljö som kontinuerligt och automatiskt uppdateras avseende säkerhet. Varje ny säkerhetspatch utvärderas av Axians speciallister och testas i isolerade labbmiljöer. Därefter godkänns de för produktion och installeras på berörda system.

Förutom att uppdatera servern så garanterar Axians att servern är tillgänglig dygnet runt och året om med Axians 24/7/365-organisation som övervakar servern och hanterar alla typer av incidenter.

FÖRVALTA BEHÖRIGHETER

- OCH ANVÄND STARKA AUTENTISERINGSFUNKTIONER SAMT BEGRÄNSA OCH SKYDDA BEHÖRIGHETER

MSB säger: För att förhindra att en angripare kan använda sig av existerande konton som finns i it-miljön behöver organisationen ha kontroll på konton och tilldelade behörigheter. En viktig del är att ha starka autentiseringsfunktioner samt att vara medveten om att lösenord ofta är en sårbarhet som en angripare gärna utnyttjar.

Axians lösning: Som kund hos Axians finns alltid en dokumenterad process för administration av åtkomsträttigheter som ger åtkomst till Kundens informationstillgångar eller IT-resurser. Alla åtkomst-rättigheter ska skriftligen godkännas (på papper eller elektroniskt) av behörig person innan de tilldelas en användare.

Behörigheter tilldelas endast personer med ett faktiskt behov, och enligt principerna om åtskiljande av arbetsuppgifter och minsta möjliga behörighet. Behörigheten avslutas utan dröjsmål när detta behov inte längre föreligger. Tilldelade behörigheter följs upp regelbundet genom en dokumenterad genomgång med bekräftelse på att behörigheten fortfarande är relevant och korrekt. Inaktuella behörigheter tas bort.

Alla behörigheter/accesser ska vara individuella. Gruppkonton tillåts endast efter separat överenskommelse mellan Axians och våra kunder.

All användning av gruppkonton redovisas till kunden, minst kvartalsvis. Lösenord för konton som används av flera individer måste lagras krypterat med spårbarhet på personnivå när ett lösenord har lästs/använts.

Många informationssystem kräver systemkonton med justerade behörigheter, men exakt vilka behörigheter som krävs är ofta dåligt dokumenterat av leverantören. Detta leder till att konton tilldelas alltför höga behörigheter för att underlätta att informationssystemet ska fungera direkt efter installationen. Angripare utnyttjar detta för att utöka sin åtkomst.

För att minska risken att en angripare kan nyttja användar- och systemkonton med höga behörigheter så säkerställer Axians att tilldelningen och användningen av dessa behörigheter begränsas i så stor utsträckning som möjligt.

Axians har stödsystem som säkerställer att processerna på ett automatiskt sätt efterlevs och hindrar att manuella felaktiga rättigheter kan delas ut. Därmed kan Axians säkerställa att endast rättigheter som behövs är utdelade vid rätt tid.

INAKTIVERA OANVÄNDA TJÄNSTER OCH PROTOKOLL

MSB säger: För att minska exponeringen ska informationssystem ha så få aktiva tjänster, protokoll och nät-verkskopplingar som möjligt. De tjänster, protokoll och nätverkskopplingar som inte behövs för informationssystemets funktion ska stängas av, tas bort eller blockeras.

Axians lösning: Som ett tillägg till Axians ”OS Management”-tjänst kan du som kund till Axians även aktivera tjänsten ”Windows Serverhärdning”. Det är en tjänst som garanterar att dina operativsystem säkras ytterligare genom serverhärdning. I tjänsten övervakar Axians att dina servrar är härdade enligt ett visst regelverk, om den bestämda konfigurationen inte är aktiv så går ett larm och Axians kan på ett proaktivt sätt säkerställa att dina servrar går tillbaka till den godkända konfigurationen. Tjänsten ger dig som kund en möjlighet att automatiskt säkerställa att du lever upp till ställda krav på compliance och säkerhet.

SÄKERHETSKOPIERA

MSB säger: För att kunna återställa förlorad eller felaktigt ändrad information eller systemkonfigurationer behöver organisationen göra säkerhetskopior och ha en förmåga att läsa tillbaka informationen från dessa.

Axians lösning: Axians tjänst för dataskydd innebär att regelbunden backup tas av dina informations-tillgångar.

Säkerhetskopiering sker normalt en gång per dygn och säkerhetskopian skapas och förvaras alltid fysiskt på annan plats än där kundens produktionssystem finns.

Återläsning av data är enligt Axians standardpolicy möjligt 30 dagar tillbaka men Axians kunder kan själv välja att göra avsteg från både lagringstider och backup-schema vid behov. Datat kan krypteras för att ytterligare höja säkerheten och vid behov kan Axians även automatisera skapandet av ytterligare en säkerhetskopia som kan skickas till valfri annan plats, t.ex. en lagringslösning i det publika molnet. All data som kopieras och exporteras på det sättet krypteras av Axians.

TILLÅT ENDAST GODKÄND UTRUSTNING I NÄTVERKET

MSB säger: För att motverka att obehöriga enheter som ansluts till nätverket får åtkomst till organisationens informationssystem och tjänster behöver organisationen aktivt inventera och upptäcka nya enheter. Organisationen behöver också agera så att endast godkända enheter ges åtkomst till tjänster och informationssystem.

Axians lösning: Axians hanterar denna utmaning i två olika lägen där det initialt handlar om att säkerställa att icke-godkända enheter aldrig ska kunna ansluta sig till nätverket. Detta gör vi bland annat med ett ”zero-trust-baserat” designtänk, lösningar med nätverksåtkomstkontroll och certifikatbaserade anslutningar till nätverket.

Om det däremot funnits brister i kontrollen av vilka enheter som är anslutna till nätverket kan Axians Vulnerability Scanning-tjänst vara en stor del av lösningen för att säkra upp din IT-miljö.

Axians Vulnerability Scanning-tjänst är ett automatiserat verktyg som identifierar och klassificerar sårbarheter i datorer, nätverk och applikationer genom att matcha dem mot redan kända systembrister. Det kan till exempel röra sig om saknade patchar och gamla protokoll, certifikat med svag kryptering eller dåliga skiffer och tjänster. Kritiska sårbarheter och brister hanteras, dokumenteras och följs upp på ett professionellt sätt.

Utöver detta innefattas i tjänsten även riskbedömningar av funna sårbarheter och brister, allt för att kunna säkerställa att din verksamhet har en tillgänglig och säker IT-miljö.

SÄKERSTÄLL ATT GODKÄND MJUKVARA ANVÄNDS

MSB säger: För att motverka att obehörig och otillåten mjukvara körs i organisationens informationssystem behöver det finnas säkerhetsåtgärder aktiverade. Detta skydd bör bestå av så kallad vitlistning som hindrar att otillåtna mjukvaror körs samt användningen av ett modernt operativsystem som har förmåga att ställa krav på signerad mjukvara och skript.

Axians lösning: Axians säkerställer att endast godkänd mjukvara kan användas genom att arbeta med vitlistning av applikationer med verktyg som Microsofts ”Applocker”. Som komplement till detta finns i Axians centrala brandväggstjänst en möjlighet implementera ”Applikationskontroll” för att dels kunna optimera nätverket utefter användarnas applikationsanvändning, dels för säkerhetsaspekten där du kan blockera icke-önskad användning av applikationer och på så sätt minska risken för spridning av skadlig programvara.

UPPGRADERA MJUK- OCH HÅRDVARA

MSB säger: Byt ut och ersätt föråldrad hård- och mjukvara för att motverka sårbarheter som över tiden exponerats och för att få avsedd funktion och tillräcklig säkerhet.

Axians lösning: Samtliga delar av Axians centrala plattforms-komponenter inom nätverk och kommunikation (brandvägg, lastbalanserare, Internet) och inom Axians kapacitetsplattform (backup, lagring, hypervisor) förvaltas och livscykelhanteras som en del av Axians standarderbjudande. Det innebär i praktiken att Axians som en del av förvaltningen av våra kunders mest grundläggande och kritiska infrastruktur utför följande:

- Funktionsuppdatering
- Säkerhetsuppdatering
- Livscykelhantering
- Kapacitetsplanering
- Kontinuitetstester
- Sårbarhetsanalyser
- Riskanalyser

Allt detta sker i bakgrunden helt utan extra kostnad och helt utan en arbetsinsats från våra kunders IT-avdelningar.

SÄKERSTÄLL FÖRMÅGA ATT UPPTÄCKA SÄKERHETSHÄNDELSER

MSB säger: Skaffa förmågan att upptäcka säkerhetshändelser i IT-miljön så tidigt som möjligt. Övervaka händelser i it-miljön med manuella, tekniska och automatiska åtgärder. Skapa säkerhetsloggar som kan användas för övervakningen och som skyddas mot obehörig åtkomst eller förändring.

Axians lösning: För att du som kund till Axians skall känna dig trygg erbjuder Axians en rad tjänster inom olika områden som på ett proaktivt sätt skyddar och informerar om aktuella hotbilder av olika slag. Axians infrastruktur övervakas och har central loggning för att säkerställa att eventuella avvikelser fångas upp.

I våra brandväggar kan vi aktivera följande funktioner:

- System för intrångsskydd (IPS/IDS)

  Upptäcker och förhindrar avancerade hot, botnät och riktade attacker mot nätverket.

- Antivirus i brandvägg

  Tjänsten ökar skyddet mot malware-varianter och kan med proaktiv teknik blockera tidigare okända hot.

- Surf-filter

  Webbfiltreringstjänsten ger våra Kunder god möjlighet att implementera noggrann kontroll för inkommande och utgående kommunikation. Tjänsten erbjuder även möjligheten att ha full kontroll över hur slutanvändaren får tillgång till webbinnehåll på internet. Tjänsten ökar skyddet mot de senaste varianterna av hot genom policybaserade kontroller med mycket detaljerad blockering och filtrering.

- Applikationskontroll

  Att kunna blockera icke-önskad användning av applikationer kan minska risken för spridning av skadlig programvara.

Utöver dessa funktioner har Axians många säkerhetstjänster för att anpassa och optimera säkerheten beroende på behov. Ett exempel på detta är en "Web Application Firewall" för att ytterligare tillföra säkerhet för publikt publicerade applikationer.

Trafikflödet i din IT-miljö övervakas även dygnet runt för att detektera intrångsförsök, loggning sker likaså dygnet runt och sparas på sådant sätt att hotaktör ej kan komma åt dom.

Axians säkerhetsavdelning övervakar både servrar och klienter med en Next-Gen Antivirus-lösning från SentinelOne. Vid inkommande incidenter kommer våra experter inom området snabbt vidta åtgärder för att säkerställa att er verksamhet löper på, riskfritt och störningsfritt.

SEGMENTERA NÄTVERKEN

MSB säger: Upprätta olika nätverkssegment och skapa kontrollerade trafikflöden mellan segmenten med hjälp av filtreringsfunktioner som skyddar mot att oönskad trafik kan flöda fritt i nätverket.

Axians lösning: Som kund hos Axians har du i de flesta fallen fått hjälp med både design och implementation av ditt nätverk och då har det alltid funnits ett ”security by design”-tänk i alla lager. Det vill säga hela kedjan från hur du ansluter dig till våra datacenter till konfiguration av centrala brandväggar, lokala brandväggar och den nätdesign som dina applikationer och system sen rullas ut på. Att arbeta med segmentering innebär att du får kontroll över dina trafikflöden och det är en självklarhet för oss att göra på det sättet när vi implementerar våra lösningar.

SLUTORD

Axians tar alltid ett helhetsansvar för att vår leveransplattform är säker och stabil. Fast ovanpå den plattformen har våra kunder en stor frihet i hur man väljer att designa sina lösningar och här krävs ett tätt samarbete mellan Axians och våra kunder. Något vi alltid eftersträvar.

Att ha en IT-lösning på Axians plattform innebär alltid ett delat ansvar för IT-säkerheten och här är det ofta upp till våra kunder hur de väljer att hantera säkerheten. Vi kommer alltid att komma med rekommendationer och våra olika tjänster ger ett skydd mot de flesta typer av hot, fast det är i slutändan alltid kunden som väljer vad Axians ska göra och vad man vill göra själv.

Skulle du vilja veta hur vi kan stötta er verksamhet? Eller har du några andra funderingar? Tveka inte att mejla oss på info.axiansse@axians.com så hör vi av oss omgående eller kontakta en av våra kundansvariga direkt.

FABIAN DAHLBERG
Sales Manager
fabian.dahlberg@axians.com
+46 (0)73 231 26 73

FREDRIK KARLSSON
Sales Executive
fredrik.karlsson@axians.com
+46 (0)73 870 41 49

Läs gärna mer om oss på www.axians.se