advenica

Säkra kommunens digitala kommunikation

Cybersäkerhet för kommuner

Cybersäkerhet – ert ansvar gentemot era invånare

Ransomware-attacker mot kommuner och liknande organisationer är vanligare än någonsin. Attackerna kan blockera alla datorer, och därmed all digital kommunikation. Angriparen kanske även kräver en stor lösensumma för att låsa upp dem. Att undvika digital kommunikation är knappast ett alternativ i dagens värld och det enda sättet att undvika att falla offer för dessa attacker är att arbeta med cybersäkerhet på ett konsekvent och strukturerat sätt.

Digital kommunikation – snabb, lätt och riskfylld

Med en större digitalisering ansluts fler enheter till Internet – bekvämt, men detta ökar också de möjliga attackvägarna in i IT-strukturen. Samtidigt blir de metoder som används av dagens angripare mer och mer förfinade och attackerna idag är oftast riktade och välplanerade.

Miljoner av anledningar att investera

I april 2019 infekterades cirka 10 000 av kommunens datorer i Baltimore, Maryland (USA) med "fillåsande" ransomware. Hackarna krävde en lösensumma på 13 bitcoin (ca 100 000 USD), men staden vägrade att betala.[1] Attacken gjorde det omöjligt att använda kommunala betalnings- och ekonomisystem. Effekten

1 Baltimore government held hostage by hackers' ransomware från https://www.bbc.com/news/technology-49393479

blev att hus inte kunde säljas, räkningar inte betalas etc. samtidigt som stadsnäten stängdes ner. Borgmästaren uppskattade den pågående skadan till över 18 miljoner USD, inklusive "8 miljoner USD förlorade på grund av uppskjutna eller förlorade intäkter medan staden inte kunde behandla betalningar."

Lake City, en liten stad i Florida, drabbades av en katastrofal attack med skadlig programvara i juni 2019. Trots att stadens IT-personal kopplade bort drabbade system inom tio minuter efter att attacken upptäcktes, infekterade en ransomware-stam nästan alla stadens datorsystem. Det enda undantaget var polisens och brandkårens system som kördes på ett separat nätverk. Ett krav på lösensumma gjordes en vecka efter infektionen, där hackare kontaktade stadens försäkringsleverantör som förhandlade fram en lösensumma på 42 bitcoins (480-500 000 USD).

> ***... minst 170 myndighetssystem i län, städer eller delstater har attackerats sedan 2013***

Allt fler attacker – och väldigt kostsamma

Dataintrång ökar ständigt. Enligt CNN har minst 170 myndighetssystem i län, städer eller delstater attackerats sedan 2013.[2] Och som Baltimore och Lake City vet kan ett dataintrång bli mycket dyrt. Ett annat exempel är det danska rederi- och oljebolaget Maersk som 2017 drabbades av en enorm cyberattack, som nästan fick bolaget att försvinna från marknaden. Den attacken kostade företaget cirka 300 miljoner USD i förlorade intäkter. Dessutom behövde hela IT-strukturen installeras om.

2 Crippling ransomware attacks targeting US cities on the rise från https://edition.cnn.com/2019/05/10/politics/ransomware-attacks-us-cities/index.html

Ny lagstiftning – högre krav på informationssäkerhet

NIS-direktivet har en rad nät- och informationssäkerhetskrav som gäller för operatörer av väsentliga tjänster och leverantörer av digitala tjänster. Eftersom det är ett EU-direktiv måste varje EU-medlemsstat anta nationell lagstiftning som följer eller "transponerar" direktivet. Direktivet syftar till att uppnå en hög gemensam säkerhetsnivå i nätverk och informationssystem för kritiska samhälleliga och digitala tjänster inom unionen. På så sätt blir den inre marknaden starkare och de centrala socialtjänsternas sårbarhet minskar.

SecuriCDS datadioder

SecuriCDS Data Diode förhindrar inte bara intrång och upprätthåller nätverksintegritet utan förhindrar lika effektivt läckage och upprätthåller nätverkskonfidentialitet. Denna lösning med hög säkerhet skyddar tillgångar för operatörer inom bland annat kritisk infrastruktur, kommuner eller försvarsindustrin. SecuriCDS Data Diode garanterar enkelriktad åtskillnad mellan nätverksgränssnitt och kan säkert ansluta två nätverk av samma eller olika säkerhetsnivåer.

Fördelar

- Skapar enkelriktad loggtrafik från övervakade system till loggsamlingssystemet
- Eliminerar dataläckage från loggdatasystemet, samt attackerares möjlighet att hoppa mellan system
- Aktiverar strikt segmentering medan central övervakning av system och nätverk behålls
- Gör det möjligt att använda ett enda system för datainsamling av loggar utan att äventyra säkerheten - detta minskar kostnaderna, ökar administratörens insikt och förbättrar möjligheten att upptäcka attacker och snabbt vidta motåtgärder

Advenica SecuriCDS Data Diodes

Hur ni håller era medborgares integritet och integritet säker

Advenica hjälper kunder att identifiera sårbarheter i nuvarande hårdvara och nätverkskomponenter. Utifrån detta ger vi råd om hur man kan vidta strategiska och effektiva åtgärder mot högre informationssäkerhet. Våra 20 års erfarenhet av cybersäkerhetslösningar gör att vi kan ge råd om den bästa vägen utifrån era behov gällande informationssäkerhet. Vi hjälper statliga myndigheter, landsting och kommuner att skydda sekretessbelagda uppgifter och hålla igång sin infrastruktur. Våra lösningar hjälper er också att uppnå efterlevnad av GDPR, NIS och säkerhetsskyddslagstiftning.

Ställ högre krav på informationssäkerhet

Kontrollera att säkerheten är inbyggd i systemet ...

Komplexa nätverk och ökat beroende av nätverksbaserade tjänster ökar behovet av högre säkerhets- och kvalitetsnivåer. För att få detta krävs robusta system och tillgång till säkerhetslösningar som skyddar informationen och säkerställer att data inte går förlorad. Tyvärr är användare vanligtvis inte särskilt bra på säkerhetskrav när det kommer till datorer, applikationer och system anslutna till internet. Det är därför av största vikt att ha med informationssäkerhet redan från början när man skriver kravspecifikationer för ny teknik, genomför upphandling av ny teknik eller inleder dialog med potentiella leverantörer. Det allvarligaste problemet är ofta att befintliga, kanske föråldrade, system och nätverk utgör det allvarligaste hotet mot IT-säkerheten. All äldre utrustning som utsätts för anslutna nätverk bör säkerhetstestas för att upptäcka säkerhetshål. För att hantera potentiella hot mot systemen måste du tänka om kring säkerheten. Kontrollera att säkerheten är inbyggd i systemet, att systemen är säkra från grunden. På så sätt kommer informationssäkerheten inte att öka komplexiteten – istället kommer den att byggas in i basen av nätverkssystemen.

ZoneGuard

ZoneGuard erbjuder en anpassad men enkel informationspolicybaserad lösning för ett säkert informationsutbyte mellan olika säkerhetsdomäner. Som gateway använder den ett tillvägagångssätt som bygger på allowlisting, vidarebefordrar endast mottagen information som överensstämmer med informationspolicyns struktur, format, värden och digitala signaturer. Alla ändringar kräver en digitalt signerad informationspolicy av antingen en IT säkerhetsavdelning eller annan utsedd policygodkännare. ZoneGuard tillhandahåller också styrning av loggar och audit trail - vitala bevis för efterlevnad av policyer och regler.

Fördelar

- Gör det möjligt för leverantörer att stödja utrustning via remote desk protocol (RDP)
- Förhindrar riskabla, onödiga anslutningar associerade med RDP, såsom skrivare, mikrofoner och högtalare
- Förhindrar obehörig användning
- Förhindrar direkt nätverkskommunikation, vilket förhindrar att virus och ransomware sprids från webbplatsen till leverantören, och vice versa
- Ger fullständig spårbarhet - vem, vad och när
- Kan förlängas med tidsbegränsad eller schemalagd anslutning
- Möjligt att utforma en princip för tvåhandsfattning som gör det möjligt för en intern gatekeeper att bestämma hur och när anslutning är tillåten

Advenica ZoneGuard

Nätverkssegmentering – fundamentalt för informationssäkerhet

Många IT-arkitekturer bygger på system designade under en politiskt stabil era och har ofta vuxit under åren. Att få aktuell information om t.ex. elanvändning, beställning av tjänster 24/7 eller distansarbete har också blivit standard, vilket resulterat i sammankopplade SCADA-system, affärssystem och internet. För att skydda kritisk information måste strikt nätverkssegmentering tillämpas med en kombination av fysisk och logisk separation. Fysisk separation skapar säkerhetszoner som distribueras på fysiskt olika hårdvaruenheter. Logisk separation gör att olika zoner eller nätverkstrafik kan samallokeras på samma hårdvara eller nätverkskabel – mindre uppenbart och med mindre förtroende för separationsmekanismens styrka än fysisk separation. Fysisk separation ska alltid tillämpas vid separering av kritiska system som SCADA-system från mindre kritiska system, t.ex. kontorsnätverk och internet. Informationsflöden mellan säkerhetszoner måste alltid övervakas för att förhindra informationsläckage och för att skydda integriteten hos känsliga system. Certifierade lösningar som uppfyller militära standarder ger högsta nivå av säkerhet och funktionalitet.

Eliminera risken för dataläckage och manipulation

För att skydda känsliga system och konfidentiell data är Advenicas datadioder den felsäkra vägen att gå. Funktionen hos en datadiod är att tillåta all data att passera framåt, samtidigt som all data blockeras i motsatt riktning. Den fiberoptiska anslutningen gör det fysiskt omöjligt för data att färdas i motsatt riktning. Och eftersom det inte är mjukvara kan den inte direkt attackeras av skadlig kod, vilket resulterar i hög säkerhet. Varje organisation som har känslig information har stor användning av en datadiod för att skydda sin värdefulla information och säkert utbyta data.

Minska hoten kring fjärråtkomst

För att ytterligare minska potentiella attackvektorer och samtidigt ge säker och selektiv åtkomst till systemen från fjärrnätverk bör en security gateway för kontrollerat informationsutbyte – Advenicas ZoneGuard – implementeras. Genom att använda ZoneGuard, med kapacitet för fjärråtkomst, kontrolleras åtkomst och hot mot en fjärråtkomstlösning minskas effektivt i gränsöverskridande domäner. All information valideras och transformeras, vilket gör att känslig information stannar inom det skyddade nätverket och skadlig kod kan inte spridas.

Säker filimport

Att importera filer till säkra miljöer är ett annat område som utgör ett betydande säkerhetshot om inte filerna saneras ordentligt före överföringen. Genom att använda Advenicas File Security Screener, en Cross Domain Solution med hög säkerhet med skanning av skadlig programvara och content disarm och återuppbyggnads-funktioner, tillhandahålls effektiva och automatiserade motåtgärder för skadlig programvara. Samtidigt säkras separation för de anslutna nätverken. File Security Screener tillhandahåller en effektiv, skalbar och pålitlig lösning för säker filimport.

File Security Screener

Att importera filer till säkra miljöer är ett annat område som utgör ett betydande säkerhetshot om inte filerna saneras ordentligt före överföringen. File Security Screener är en hög-assurans Cross Domain Solution med skanning av skadlig programvara och content disarm och återuppbyggnads-funktioner.

Fördelar

- *Scanning efter skadliga program med hjälp av tredjepartslösningar som OPSWAT MetaDefender Core och sandlådemiljöer.*
- *Advenicas datadioder med hög assurans som skydd mot informationsläckor.*
- *Separation av olika importkällor med hjälp av Advenicas datadioders höga assurans.*
- *Möjlighet för cachning av filer som ska scannas vilket tillåter att underhåll kan genomföras på systemet utan att data förloras.*
- *Anpassningsbara regler för import av filer, vilka baseras på informationskällan och filtypen.*
- *Anpassbar lösning med förmågan att öka antalet anslutna system eller ökad genomströmning.*

Advenica tillhandahåller expertis, hög assurans och cybersäkerhetslösningar i världsklass för kritisk data-in-motion upp till Top Secret-klassning. Med oss stärker länder, myndigheter och företag informationssäkerheten och digitaliserar ansvarsfullt. Bolaget grundades 1993 och har EU-godkännande på högsta säkerhetsnivå. Våra unika produkter designas, utvecklas och tillverkas i Sverige.

Läs mer på advenica.com

advenica

ISO 9001 CERTIFIED
ISO 14001 CERTIFIED