Självstudieuppgift
Dataläckage

Den här självstudieuppgiften är framtagen för att ge dig som arbetar med cybersäkerhet möjlighet att träna på att upptäcka och hantera incidenter. På första sidan finner du det övergripande scenariot med en beskrivning av miljön och av vad som har hänt. På nästa sida hittar du de uppgifter som du på egen hand löser med hjälp av de filer som tillhandahålls. Du hittar också tips som du kan använda om du kör fast, samt förslag på hur uppgifterna kan lösas.

Scenario

Unicorp har producerat mediciner till sjukvården runt om i världen sedan början av 2000-talet. Till en början fanns företaget endast i Eslöv, men har succesivt etablerat sig på fler platser i landet. Det senaste tillskottet är det nyta huvudkontoret i Lund.

Nu har en incident inträffat där produktionsdata har exfiltrerats ur organisationen via servern FTP på DMZ, sannolikt genom ett angrepp mot organisationen. Unicorp bedömer att läckan kan ge dålig publicitet för företaget, men att driften inte kan påverkas. De anställda är förvånade över att ett angrepp kan ha lyckats eftersom organisationens nätverk byggdes för att ha hög säkerhet.

IT-miljön

I företagets IT-miljö finns två domäner uppdelade på 11 stycken nätverkssegment. Den ena domänen, Unicorp2, innehåller kontor på olika orter i Sverige, ett DMZ samt ett servernät. Den andra domänen, Pharmenta2, tillhör själva produktionsnätet. Där finns bland annat fabriken, ett HMI-nät och ett SCADA-nät. Domänerna är separerade från varande, vilket innebär att de har egna användarkataloger som inte har någon trust mellan sig. Kontor och IT-system tillhör domänen Unicorp, medan produktionsdelen tillhör domänen Pharmenta. Ett undantag har dock gjorts för kontorsdatorer i fabriken i Eslöv som placerats i Pharmenta.

Produktionssystem

Produktionssystemet inkluderar system för orderläggning, SCADA-system för hantering av tillverkning, en fabrik för tillverkning samt ett system för rapportering och leverans. En kund gör en beställning på servern Weborder. Weborder skickar beställningen vidare till ProdDB, där den läses av SCADA-systemet på ProdOrder. Denna skickar till slut beställningen till Fabriken. När fabriken producerat medicinen skickas ett svar tillbaka till ProdOrder som skickar det vidare till ProdDB. I ProdDB finns data sammanställd för all producerad medicin.

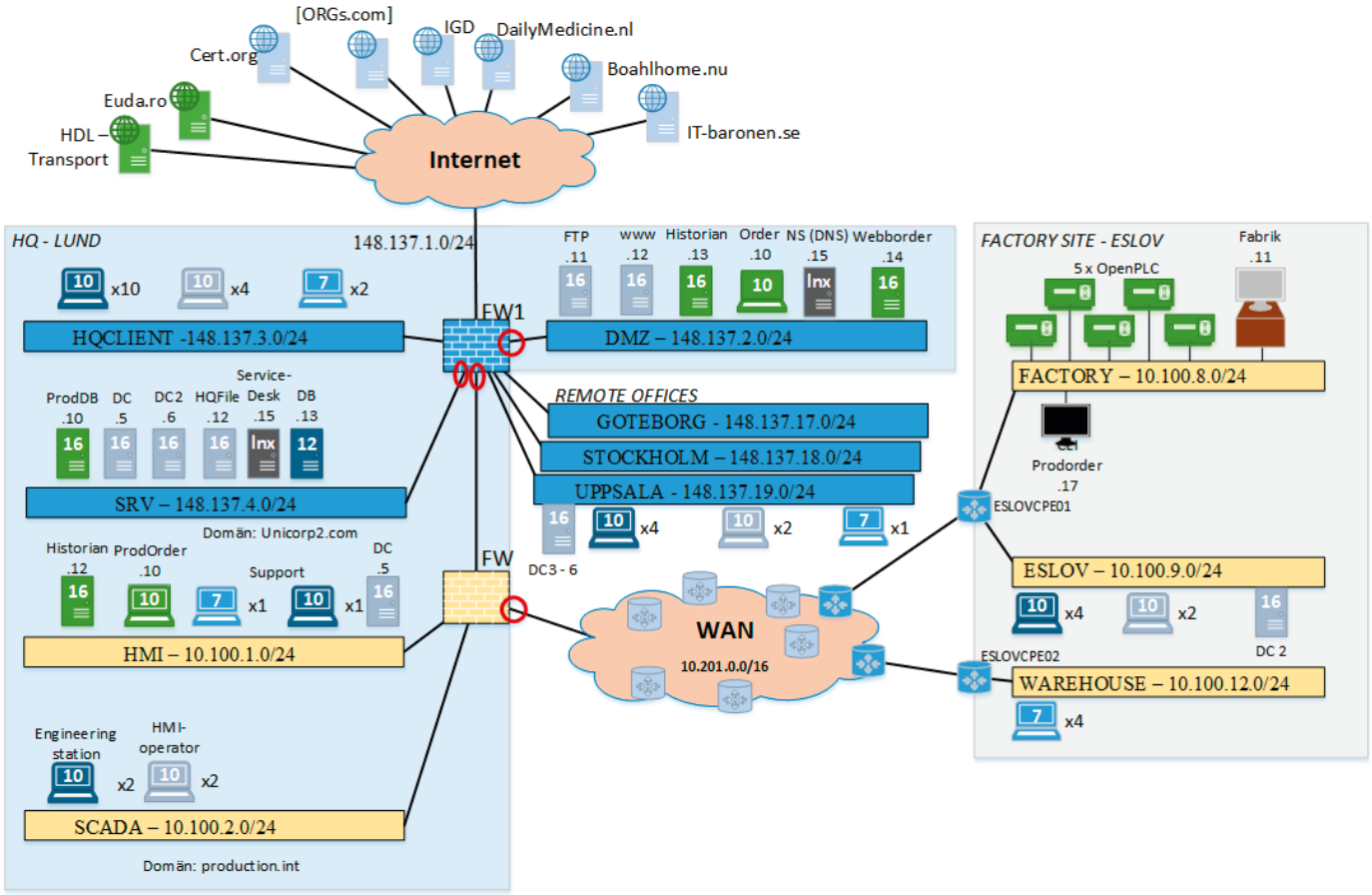
Lyckligtvis togs så kallade kape-filer[1] direkt efter att textfilen med produktionsdata (productiondata.txt) upptäcktes på FTP-servern. Säkerhetssystemen sparar också nätverkstrafiken från ett antal platser i nätverket i form av pcap-filer. Det är nu upp till dig att reda ut vad som har hänt.

På sidorna 2 – 3 finns instruktioner för uppgiften och på sidan 4 hittar du tips som syftar till att hjälpa dig hitta svaren på uppgifterna, men inte ger dig hela lösningen. På sidorna 5-7 hittar du lösningsförslag och på sista sidan hittar du svaren på frågorna i uppgifterna.

[1] https://www.kroll.com/en/insights/publications/cyber/kroll-artifact-parser-extractor-kape

Instruktioner

Huvuduppgiften är att ta reda på hur angreppet har skett. Det inkluderar att ta reda på hur antagonisten fått fotfäste i nätverket samt vilka datorer och program som har varit inblandade. Slutligen förväntas rekommendationer om vad som behöver göras för att återställa nätverken, samt för att säkra upp Unicorp mot framtida angrepp. Nedanstående bild visar organisationens nätverk. Ringarna på FW1 och FW markerar de platser i nätverket där pcap-filerna har samlats in.



Uppgiften löses genom att de kape-filer och pcap-filer som tillhandahålls i zip-filen https://download.iwlab.foi.se/uppgifter/datalackage.zip (MD5: e3acaa89979ec85c6cc1f01eaf349d43) laddas ned och analyseras. Efter det att uppgifterna lösts kan svaren kontrolleras mot ett facit som finns i under rubriken Facit i detta dokument.

Uppgift 1

Vilka datorer var inblandade i överföringen av produktionsdata till FTP-servern? Kan informationen ha läckt ut på Internet?

Uppgift 2

Analysera hur dataöverföringen skedde. Hur kunde data från ProdDB överföras? Vilka användare, processer och filer var inblandade?

Uppgift 3

Via vilka datorer tog sig angriparen in för att kunna skapa kopieringen av data från ProdDB?

Uppgift 4

Öppna zip-filen en inbäddade zipfilen Uppgift4.zip med lösenordet ”123456” i vilken det finns mer information och ytterligare en pcap. Beskriv hur antagonisten fick fotfäste i nätverken. Beskriv en tidslinje över angreppet med inblandade datorer samt hur dessa utnyttjades.

Uppgift 5

Vad behöver IT-avdelningen göra för att städa bort angreppet?

Uppgift 6

Vilka säkerhetsåtgärder hade behövts?

Återkoppla!

Din återkoppling gör det möjligt för oss att ta fram fler självstudieuppgifter. Så återkoppla gärna genom att besvara formuläret på https://survey.crate.foi.se/index.php/137482

Tips

Uppgifterna kan lösas med programmen Wireshark och NetworkMiner för att analysera nätverkstrafiken, samt något verktyg för att montera .vhdx filer. I Windows kan dessa filer öppnas direkt via filhanteraren men i Linux behöver de monteras med Guestmount. Nedan följer några exempel-kommandon för inspiration.

```
# Zippa upp fil
$ unzip unicorp-forensics.zip

# Öppna WIreshark
$ wireshark dmz.pcap

# Öppna NetworkMiner
$ mono networkminer

# Öppna kape-fil (.vhdx) för FTP servern
$ Guestmount –add ftp.unicorp2.-m /dev/sda1 –ro share/
```

Tips uppgift 1

Utgå från pcap-filerna från FW1. Öppna filerna i Wireshark eller i NetworkMiner. Samla information såsom hostnamn, IP-adresser samt aktiva nätverkstjänster för de relevanta datorerna. Fokusera på att leta efter möjliga filöverföringar och ta det vidare därifrån.

Tips uppgift 2

Sammanställ den informationen som redan är känd, såsom filnamn och aktiva nätverkstjänster. Utgå från de datorer som upplevs mest intressanta. Tänk på att produktionsdata ursprungligen bara finns på ProdDB. Leta efter intressanta artefakter. Utgå från Kapefilerna för datorer på SRV- och DMZ segmentet samt pcap-filerna från FW1.

Tips uppgift 3

Antagonisten verkar ha använt sig av en dator för att genomföra dataöverföringen. Fokusera på den datorn. Utgå från att antagonisten har fjärrstyrt datorn och fundera över hur det gick till trots att det finns brandväggar implementerade som blockerar inkommande trafik från internet.

Tips uppgift 4

Öppna png-bilden och läs textfilen från medarbetare. Utgå från dem men tänk på att medarbetaren inte känner till datorn i detalj.

Tips uppgift 5

Fundera på vad som gjorde angreppet möjligt samt vilka artefakter som antagonisten lämnat efter sig i nätverket.

Tips uppgift 6

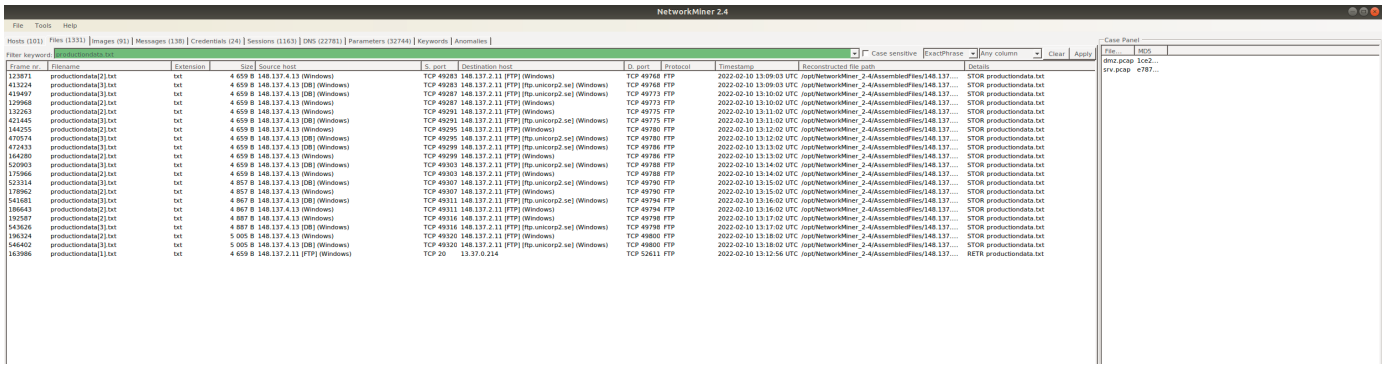
Fungera kring saker såsom nätverksdesign, systemhärdning, konfiguration av säkerhetsfunktioner samt icke-tekniska lösningar.

Lösningsförslag

I detta avsnitt presenteras förslag på lösningar till uppgifterna. Notera att det finns flera olika sätt.

Förslag uppgift 1

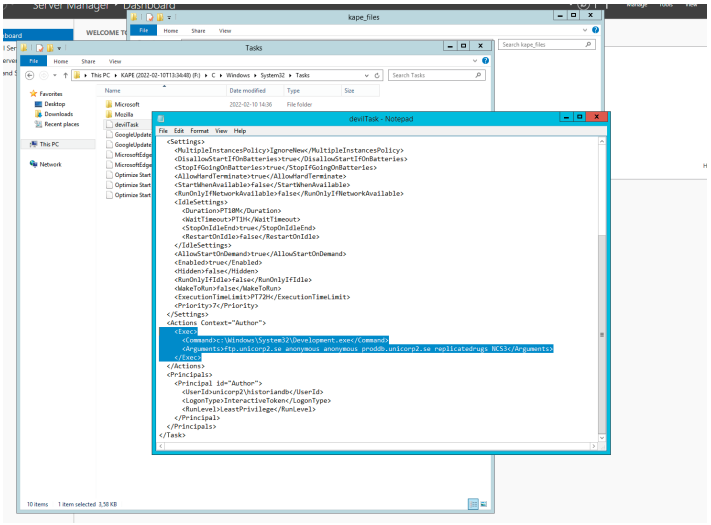
Ett enkelt sätt att lösa uppgiften på är att öppna NetworkMiner och importera dmz.pcap och srv.pcap. Navigera sen till filfliken och se vilka filer som överförts. Hitta ”productiondata.txt” som skickas mellan DB-server och FTP-servern, samt mellan FTP-servern och datorn med IP-adress 13.37.0.214.



Notera även att 1) ProddDB-servern (148.137.4.10) har port 1433 (Microsoft SQL Server) öppen, 2) DB-servern (148.137.4.13) har port 445 öppen (SMB), och 3) FTP-servern (148.137.2.11) har port 21 öppen (FTP).

Förslag uppgift 2

Klicka runt i filsystemet och sök efter jobbet ”devilTask”. Konstatera att den exekverar binären ”Development.exe” med argumentet ”ftp.unicorp2.se anonymous anonymous proddb.unicorp2.se replicatedrugs NCS3”. Detta ser ut att vara en anslutningssträng till ProdDB-servern, vilket innebär att DB-servern hämtar data från ProdDB-servern genom devilTask-jobbet, samt att produktionsdata överförs i textfilen productiondata.txt till FTP-servern.



Se även fliken ”Credentials” i NetworkMiner (srv.pcap och dmz.pcap). Där syns att användaren och lösenordet ”anonymous” har använts för att autentisera sig mot FTP-servern.

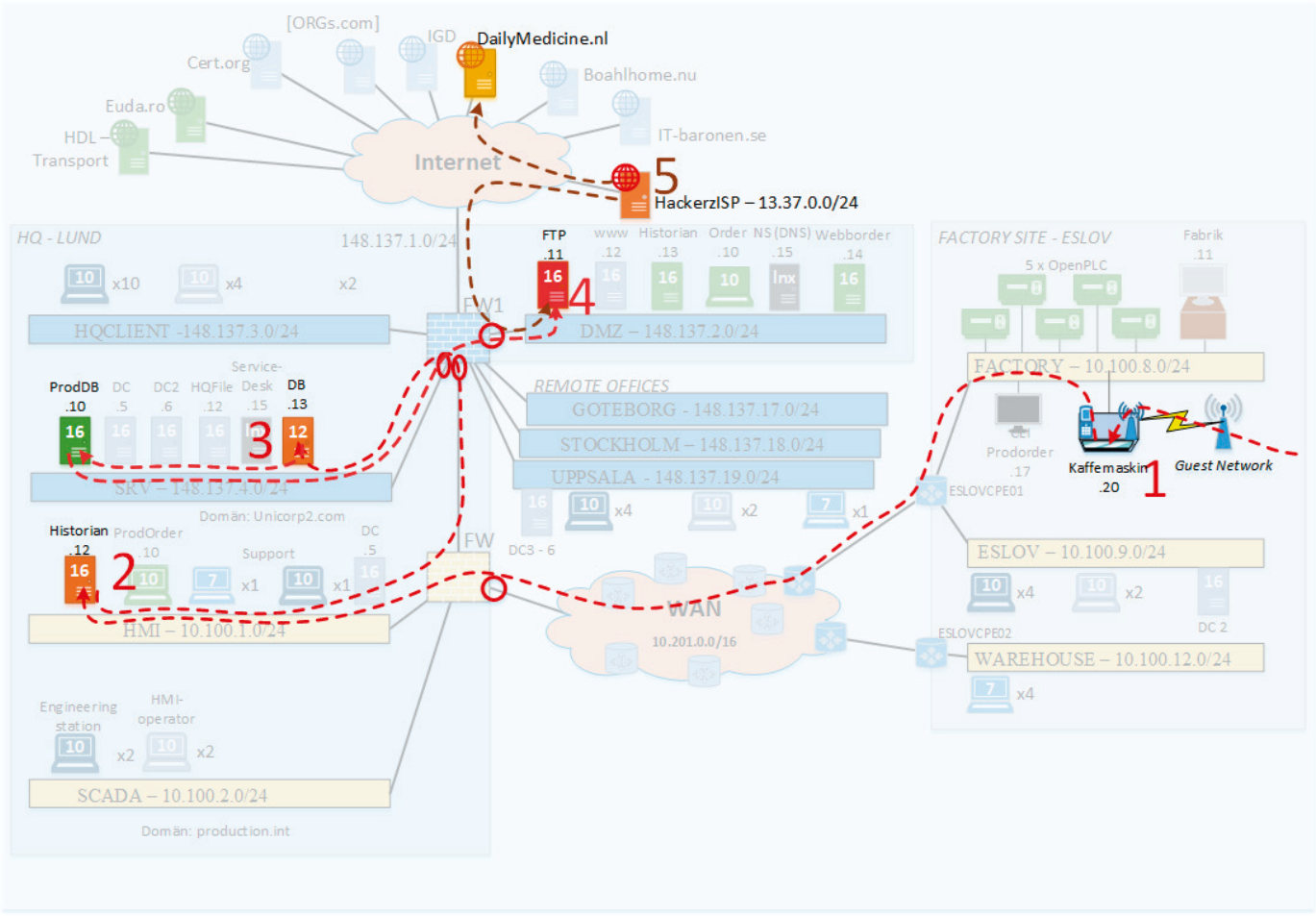
Förslag uppgift 3

Sedan tidigare är det känt att DB-servern överför produktionsdata till FTP-servern samt att DB-servern har port 445 öppen. Öppna samtliga pcap-filer i NetworkMiner. Genom att utgå från den öppna sessionen på DB-servern syns en öppen session till Historian-servern (10.100.1.12). Den servern har i sin tur en öppen session från en dator med IP-adressen 10.100.8.20.

Förslag uppgift 4

För att besvara denna uppgift behöver all data som hittills har samlats in sammanställas.
Vi vet att 5 datorer är inblandade, nämligen den med IP-adressen 10.100.8.20 samt Historian-servern, DB-servern, ProdDB-servern och FTP-servern. Med hjälp av tidsstämplar för sessionerna syns det att sessionen till Historian-servern öppnades först och sessionen till DB-servern därefter. Maskinen med IP-adress 10.100.8.20 har alltså pivoterat via Historian-servern till DB-servern och kopierat produktionsdata till FTP-servern genom att skapa jobbet ”devilTask” som exekverade ”Development.exe”. Development.exe överfördes sannolikt till DB-servern av antagonisten innan jobbet skapades.

Den sista pusselbiten svaret på hur angriparen tog sig in finns i pcap-filen i zip-filen Uppgift5.zip. I nedanstående figur visas angreppets steg tillsammans med de involverade datorerna.



I angreppets första steg utnyttjas en kaffemaskin som har anslutits till företagets produktions¬anläggning. Kaffemaskinen har två nätverkskort och därmed två IP-adresser, nämligen ”10.100.8.20” och ”79.97.24.80”. Den får automatiska uppdateringar av programvaran via leverantören ”bryggbolaget.se”. Steg 1 inleds med att angriparen tar sig in i leverantörens uppdateringsserver och byter ut uppdateringsfilen mot en version som innehåller en bakdörr. I pcap-filen ”guest.pcap” syns det att kaffemaskinen gör http-anrop till swupdate.bryggbolaget.se på port 8000 och att filen ”coffeemachine.zip” laddas ner, vilken innehåller den skadliga programvaruuppdateringen. Därefter använder angriparen bakdörren för att ansluta till kaffemaskinen och utökar sina rättigheter. Angriparen har nu etablerat fotfäste via en för företaget okänd kanal.

I steg 2 pivoterar angriparen vidare in i nätverket via kaffemaskinen till Historian-servern. Vid inloggningen på Historian-servern används en användare och ett lösenord som i ett tidigare angrepp stulits från Unicorp2. I steg 3 ansluter angriparen till DB-servern med samma användare och lösenord som till Historian-servern.

På DB-servern skapads ett schemalagt jobb som återkommande överför företagets produktionsdata från ProdDB-servern till FTP-servern. Angreppet avslutas med att en okänd användare ansluter sig till företagets oskyddade FTP-server och laddar ner kopierade produktionsdata.

Förslag uppgift 5

Se facit.

Förslag uppgift 6

Se facit

Facit

Svar uppgift 1

Productiondata.txt överfördes från DB-servern till FTP-servern. Ja, produktionsdata har läckt ut på internet till en IP på 13.37.0.214.

Svar uppgift 2

På DB-servern fanns ett jobb ”devilTask” som exekverade binären ”Development.exe” varje minut. Binären överförde produktionsdata från ProdDB-servern till FTP-servern i textfilen productiondata.txt. Jobbet ”devilTask” använde lösenordet ”replicatedrugs” för att autentisera sig mot ProdDB-servern. DB-servern använde användaren och lösenordet ”anonymous” för att autentisera sig mot FTP-servern.

Svar uppgift 3

Datorn med IP-adress 10.100.8.20 pivoterade via datorn med IP-adress 10.100.1.12 till DB-servern.

Svar uppgift 4

Datorn med IP-adress 10.100.8.20 är i själva verket en kaffemaskin. Skadlig kod laddades ner till kaffemaskinen vid en planerad uppdatering från en webbserver med IP-adress ”79.97.24.80”. Kaffemaskinen hade två nätverkskort med IP-adresserna 10.100.8.20 och 51.22.205.2.

Uppdateringen öppnade i själva verket en bakdörr på kaffemaskinen för angriparen. Angriparen anslöt till kaffemaskinen, pivoterade till DB-servern via Historian-servern, laddade upp ”Deveopment.exe”, skapade ”devilTask” och hämtade slutligen produktionsdata på FTP-servern. Se detaljer i facit för uppgift 1 och uppgift 2.

Svar uppgift 5

För att städa bort angreppet bör 1) kaffemaskinen kopplas ur, 2) produktionsdata från FTP-servern tas bort, 3) ta bort devilTask-jobbet på DB-servern, och 4) ändra så att användaren ”historiandb” har olika lösenord i domänerna unicorp2.se och production.int.

Svar uppgift 6

Generellt bör nätverkets design ses över eftersom klientdatorer är ihopkopplade med produktionsnätet. Factory-segmentet bör endast vara fysiskt ihopkopplat med HMI-nätet.

Utöver designfel finns felkonfigurationer i organisationen. För det första finns användaren ”historiandb” med i båda domänerna med samma lösenord. Detta gjorde att angriparen kunde autentisera sig mot Historian-servern och DB-servern med samma inloggningsuppgifter, trots att datorerna tillhörde olika domäner. För det andra blir inloggade användare per automatik lokala administratörer enligt gruppolicyn i domänen och det bör undvikas för vanliga användare.

Den inre brandväggen bör också konfigureras striktare genom att till exempelvis endast tillåta kommunikation mellan datorer i produktionskedjan, samt förkasta paket som inte använder tillåtna protokoll. I en produktionsmiljö som denna hade det även gått att införa autentisering av enheter med exempelvis 802.1x-protokollet, där endast autentiserade enheter får koppla upp sig till nätverket.

Slutligen bör den administrativa säkerheten i organisationen ses över. Till exempel kan en policy som säger att inga enheter får kopplas in i produktionsnätet införas. Policyer bör kombineras med utbildning som säkerställer att medarbetare förstår policyerna, samt syftet med dem.

Crate – Totalförsvarets cyberanläggning för ett säkrare Sverige

Denna självstudieuppgift är gjord med hjälp av Crate, Sveriges nationella cyberanläggning för totalförsvaret. Crate ökar totalförsvarets förmåga i cyberdomänen genom forskning, utbildning, träning, övning och utvärdering med fokus på samhällsviktig verksamhet och cyberfysiska system. Crate är ett samarbete mellan Försvarsmakten, Myndigheten för samhällsskydd och beredskap samt FOI. Läs mer om cyberanläggningen och dess verksamhet på www.foi.se/crate.

FOI Totalförsvarets forskningsinstitut

FÖRSVARSMAKTEN

MSB Myndigheten för samhällsskydd och beredskap