Myndigheten för samhällsskydd och beredskap

FAKTA

Publ.nr: MSB1091 – mars 2017

VERKSAMHETEN FÖR CYBERSÄKERHET OCH SKYDD AV SAMHÄLLSVIKTIG VERKSAMHET

Viktiga lärdomar från elavbrotten i Ukraina

Skyddet av industriella informations- och styrsystem (ICS) måste stärkas

Den 23 december 2015 meddelade ett antal ukrainska elbolag via sina webbtjänster att ett större elavbrott inträffat. De indikerade samtidigt att andra störningar förekom, såsom problem att nå kundtjänstfunktioner via telefon. Senare samma dag gick ett av de drabbade elbolagen ut med att det handlade om ett IT-angrepp som innebar att understationer kopplades bort, vilket i sin tur ledde till att kunder förlorade sin strömtillförsel. I december 2016 rapporterades om ytterligare angrepp mot elbolag i huvudstaden Kiev. Vilka lärdomar kan vi dra och vilka åtgärder borde vidtas för att upptäcka och förhindra liknande händelser i Sverige?

Det som kommit fram om de tekniska lösningarna som användes i de ukrainska bolagen pekar på att förhållandena i stort liknar de svenska. Tillvägagångssätten för intrången var inte heller nya och unika och med undantag för enstaka delar av det slutliga angreppet fanns det heller ingen programvara som användes vid angreppet som var specialgjord för elsektorn. Av det dras slutsatsen att *samtliga sektorer där industriella informations- och styrsystem används i Sverige behöver fundera på huruvida de har ett tillräckligt skydd*.

I tabellen på nästa sida ges exempel på olika säkerhetsåtgärder och aktiviteter som aktualiserats i och med händelserna i Ukraina. Tre av dessa åtgärder vill vi särskilt lyfta fram:

1. **Bättre grundskydd**. ICS-miljöer är ofta dåligt uppsäkrade ur flera perspektiv. Att införa ett bra grundskydd, i form av en IT-säkerhetsarkitektur med både tekniska och andra skydd, är något som höjer säkerheten i ICS-miljöer avsevärt.
2. **Spårbarhet och övervakning**. Idag är det alltför vanligt att ICS-miljöer inte har fullgod säkerhetsövervakning. Om man inte kan upptäcka att ett angrepp påbörjats, eller lyckats och pågått under ett längre tag kan man aldrig hantera incidenten, utreda orsak och initiala intrångsvägar.
3. **Medvetandehöjning och övning.** En förutsättning för framgångsrikt säkerhetsarbete är medvetenhet och grundförståelse för hur ICS-miljöer är utsatta för hot. Medvetenhet måste finnas på alla nivåer i en organisation, såväl driftspersonal som ledning och beslutsfattare. Organisationer måste utbilda personal samt öva hantering för att kunna förebygga och hantera IT-attacker.

Vad är känt om de attackerade systemen i Ukraina?
Någon känd samlad öppen information över vilka systemlösningar som användes i de ukrainska bolagen finns inte tillgänglig. Det går dock dra en del slutsatser utifrån öppna källor.

I en amerikansk US-CERT-varning finns information om systemens människa-maskin-gränssnitt (HMI). Denna väg användes för att stänga av strömmen. Åtminstone tre skilda sådana produkter förekom hos de olika elbolagen - GE Cimplicity, Advantech/Broadwin WebAccess samt Siemens WinCC. Detta är moderna standardprodukter som används inom olika branscher och företag runtom i världen. Produkterna bygger på Microsoft Windows-plattformar, vilka även de används över hela världen.

I en rapport från E-ISAC och SANS nämns även angrepp mot andra IT-komponenter, som realtidsenheter (RTU), kommunikationsutrustning (seriell till ethernet-konverterare), servrar och reservkraftsystem. Dessa komponenter angreps för att försvåra utredning och återställning av elleverans.

Ur ett riskperspektiv är det viktigt att understryka att de drabbade ukrainska elbolagen använde kända leverantörers produkter samt hade av varandra oberoende systemutformningar och lösningar.

Mer information:
https://ics-cert.us-cert.gov/

https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf

Mer information om säkerhet i industriella inforamations- och styrsytem finns på www.msb.se/ics

Typ av säkerhetsaktivitet	Exempel eller anledning
Proaktivt, processer och rutiner: **Medvetandehöj för bättre säkerhetskultur**	Öka medvetenheten hos medarbetare och beslutsfattare om moderna attackmetoder och social ingenjörskonst, attacker mot leverantörsled och tredjepart etc.
Proaktivt, tekniskt skydd: **Inventera IT-miljö, förstå uppsättning av utrustning**	Genom att aktivt inventera, granska och tekniskt prova hur nätverket är uppsatt, vilka in- och utgångar som finns i nätet, vilken utrustning som är anslutet samt vilka tjänster som är tillgängliga så kan organisationen bättre förstå de tekniska förutsättningarna och hotbilden. Detta arbete är underlag för IT-säkerhetsarkitektur och andra aktiva åtgärder.
Proaktivt, tekniskt skydd: **Utforma en IT-säkerhetsarkitektur**	• Använd olika säkerhetskomponenter som skapar säkerhet på applikations-, system- och nätverksnivå. • Tillämpa zonindelning, segmentering och isolering av olika typer av system baserat på användningstyp och säkerhetsklassningar. • Tillse god separation mellan olika kommunikationslösningar, exempelvis att nätverksanslutna försörjningssystem (som reservkraft) inte är direktåtkomlig på LAN utan bara från särskilda managementnät. • Se till att fjärråtkomstlösningar för distansåtkomst in till företaget i allmänhet, och till processkontrollnät i synnerhet, är utformade med stor säkerhet.
Proaktivt, tekniskt skydd: **Bygg motståndskraft mot attacker**	• Härda system, både vanliga IT-plattformar men även specialutrustning, såsom PLC, RTU, kommunikationsgateways, industriella switchar etc. • Tillämpa vitlistning av applikationer.
Proaktivt, tekniskt skydd: **Tillämpa stark autentisering**	Vid Ukrainaincidenten stals lösenord och autentiseringsinformation. Använd tvåfaktorsautentisering för att förhindra eller försvåra möjligheten för någon att stjäla och använda konton och autentiseringsuppgifter.
Proaktivt och reaktivt, processer och rutiner: **Uppdatera systemprogram och programvaror till senaste version**	De drabbade elbolagen i Ukraina visade sig använda gamla versioner av kontrollsystemsprogramvaror som innehöll kända säkerhetshål. Att inte stänga till allmänt kända säkerhetsproblem ger angripare övertag. Även programvaror i infrastrukturkomponenter, såsom nätverksswitchar måste underhållas, vilket ställer särskilda krav på nätets utformning utifrån tillgänglighet.
Proaktivt och reaktivt, processer och rutiner: **Ta fram incidenthanteringsrutiner och prioritering av larmnivåer**	Planera och dokumentera olika rutiner för användning i samband med incidenthantering.
Proaktivt och reaktivt, tekniskt skydd: **Skapa tekniska förutsättningar för att kunna utföra IT-incidenthantering och IT-forensik**	Se till att ha exempelvis färdiga möjligheter i switchar/nättappar för att kunna ansluta nätverksanalysatorer på strategiska platser.
Reaktivt, processer och rutiner: **Skapa procedurella förutsättningar för att senare kunna utföra IT-incidenthantering och IT-forensiska utredningar**	• Spara loggar tillräckligt länge, så att det går att gå tillbaka tillräckligt långt i tid för att göra en bra utredning. Ofta behövs backuper som innehåller information från åtminstone två år bakåt i tiden. • Ha rätt information sparad i backuper, så att denna inte bara kan användas för att återskapa förlorad data utan även kan användas för jämförande analys av filer i en forensisk situation.
Reaktivt, processer och rutiner: **Tillse fullgod nätverks- och säkerhetsövervakning som i tid upptäcker anomalier**	• Tillse upptäckt av onormala näthändelser i form av ovanligt stora trafikvolymer (t ex dataexfiltration), nya informationsflöden och ovanliga trafikriktningar, tidigare ej använda protokolltyper mm. • Tillse upptäckt av säkerhetshändelser i form av att brandväggar blockerar och larmar på en oförväntad uppkoppling, t ex från ett internt nät ut mot internet. • Tillse upptäck av onormal användning av olika typer av användarkonton, t ex sådana VPN-inloggningar som inte bör förekomma såsom administratörsinloggningar som sker utan att behörig IT-administratör kan ha utfört dem.
Reaktivt, tekniskt skydd: **Tillse tekniska lösningar för att spara och bearbeta säkerhetslarm och säkerhetsloggar**	Tillse att det finns dedikerade system för centraliserad larm- och loggmottagning samt larm och loggbearbetning på ett sådant sätt så att spårbarhet av aktiviteter på olika delar av infrastrukturen erhålls.

Faktabladet är framtaget av Programmet för säkerhet i industriella informations- och styrsystem i samarbete med Robert Malmgren.

Kontakta Myndigheten för samhällsskydd och beredskap

MSB 651 81 Karlstad

Tfn: 0771-240 240
Fax: 010-240 56 00

registrator@msb.se
www.msb.se

Kontaktpersoner:
Kristina Blomqvist
kristina.blomqvist@msb.se
Anders Östgaard
anders.ostgaard@msb.se