Uppgiftens innehåll och genomförande

API-säkerhet i B2B och B2C

Skillnader i autentisering och kryptering

- Starkare personlig verifiering vid B2C (t.ex bankid)
- B2B använder fler certifikat och nycklar
- B2C har högre krav på skydd gällande personuppgifter

Regelverk som påverkar

- NIS2: Fokuserar på driftsäkerhet, leverantörsrisker och incidenthantering
- GDPR: Starkast påverkan på B2C personuppgifter, incidentrapportering
- CER:Säker design, patchning och incidenthantering för båda.

Viktigaste skyddsåtgärder

- Verifiering av identitet.
- minsta möjliga behörighet
- Bra kryptering i transit och vila.
- Övervakning och loggar som bevakar vem som begär information.

> Reflektion: Varför skiljer sig kraven mellan B2B och B2C?
>
> Kraven skiljer sig eftersom B2C-API:er hanterar personuppgifter och exponeras mot en stor och okänd användarbas, medan B2B-API:er bygger på avtalade relationer men ofta är mer affärs och samhällskritiska. Detta leder till olika hotbilder, risknivåer och regulatoriska krav.

Sammanfattning - syfte, metod, viktiga slutsatser

Syfte:

- Att vi som grupp ska planera och utföra en riskworkshop åt ett fiktivt företag
- Att kunna identifiera risker inom kritiska samhälls
- Att kunna samarbeta för att göra en stor uppgift tillsammans
- Lära sig hitta vilka artiklar som gäller verksamheten man jobbar på.

Metod:

- Vi utgick mest från MSB:s metodstöd
- För att hitta individuella hot använde vi även STRIDE

Viktigaste Slutsatser:

- Man kan alltid förbättra ett system
- Det finns många regelverk som kritiska verksamheter ska ha koll på, men många av dem går in i varandra.
- Man måste vara flera personer för att få flera perspektiv för att kunna lista ut alla problem i ett system eller hot

Sammanfattning för ledningsnivå

Efter vår riskbedömning så finns det vissa saker som måste bli tittade på men som man lätt kan åtgärda för att minska risknivån för intrång i systemen. Det finns även flera områden man kan förbättra för att göra systemet mer robust för att minska incidenter inom systemet. Det kommer kosta tid och pengar för att få ihop allt.

Generellt är det bra uppfyllning av krav gällande regelverken men det är viktigt att man säkerställer att det följs som det ska. Det finns även en bra grund för IT-säkerheten inom Nordlunda men det finns mycket man kan förbättra för att säkerställa verksamheten långsiktigt. En säkerställning av logghanteringen och utbildning av personal är lösningar som bör åtgärdas.

Övergripande bedömning av risknivå

Risknivå

- Medel, Detta är på grund av dålig loggning + att personal inte är utbildade och att konton inte följer least privilege

Riskområden

- Styrsystemen
- Ekonomi Sektorn

Regulatoriska brister

- Det behövs flera krav inom NIS2, Elsäkerhetslagen, GDPR och DORA är endast delvis uppfyllda.
- Största brister finns inom riskhantering, incidentrapportering, leverantörsstyrning och dokumenterad säkerhetsstyrning.

Prioriterade åtgärder

- Förbättrad loggning för att upptäcka och registrera problem och hot.
- Kontinuerlig utbildning för personalen i syfte att undvika phishing och spoofing.
- Ökad redundans i driften.

Nordlunda Energi AB är ett energibolag som hanterar elnätverk och fjärrvärme i orten Nordlunda. Kärnverksamheten går ut på att leverera el och fjärrvärme till kunder. Det står även för planering av elnätet och underhåll av det. Deras huvudsakliga mål är elsäkerhet, värme åt kunder vid vintertid, snabb incident response och efterlevnad av lagar.

Inom IT-miljön finns det många kritiska tjänster som ekonomisystem, kundsystem och affärssystem.

Processerna som är starkt beroende av OT-systemen är SCADA, driftövervakning, elcentral, styrsystem, distribution och mätvärdeshanteringen. Själva driften av verksamheten är starkt beroende av att OT-system är igång och fungerar.

Högt beroende av OT för temperaturstyrning, pumpar, ventiler och övervakning.

IT-systemen är mer kritiska när det gäller fakturering, kundtjänsten, ekonomi och affärssystem, de mer interna funktionerna och kundgränssnitten.

För kommunikation mellan stationer används Sahala nätverket. Det finns även redundanta anslutningar till driftcentralen och datacenter.

Det finns en CISO som ansvarar för arkitekturen och riskhantering över nätverken och en OT-ansvarig. Det finns även en SOC via en MSSP som hanterar cybersäkerheten.

Kundgrupper

Privatpersoner
Försörjer hushåll med el, värme och nätanslutning. Kunden är volymmässigt stor och känslig för längre driftstörningar, vilket påverkar förtroende och varumärke.
Kommunala verksamheter:
innefattar skolor, vård- och omsorgsverksamheter, fastighetsbolag och tekniska förvaltningar. Dessa aktörer är beroende av stabil energiförsörjning och tydliga kommunikationskanaler vid incidenter.

Industriella aktörer:
Produktionsintensiva företag med höga krav på kontinuerlig energitillgång, ofta med egna automations- och styrsystem. Driftavbrott kan leda till betydande ekonomiska konsekvenser och krav på snabb återställning.

Kritiska samhällsfunktioner:
Exempelvis räddningstjänst, sjukvård, vattenförsörjning och transportinfrastruktur. Dessa verksamheter kräver högsta nivå av tillgänglighet, redundans och incidentberedskap då störningar kan få direkt påverkan på liv, hälsa och samhällsstabilitet.

Sammanfattning av regulatorisk kartläggning

Den regulatoriska kartläggningen har genomförts för att identifiera vilka regelverk som är mest kritiska för Nordlunda Energi AB samt hur väl organisationen uppfyller kraven i dessa. Kartläggningen visar att verksamheten omfattas av flera regelverk samtidigt och att många av kraven överlappar varandra. Brister inom ett område påverkar därför ofta efterlevnaden av flera regelverk.

Det kritiska regelverket för Nordlunda Energi AB är NIS2. Enligt kartläggningen är ett av kraven inom NIS2 helt uppfyllt, medan majoriteten av kraven är delvis uppfyllda. De delvis uppfyllda kraven gäller främst områden som riskhantering, loggning, leverantörsstyrning, utbildning och incidenthantering. Flera krav, bland annat kopplade till incidentrapportering och dokumenterad spårbarhet, bedöms som ej uppfyllda, vilket innebär en tydlig regulatorisk risk.

GDPR är också ett centralt regelverk, framför allt kopplat till kundsystem, fakturering och andra system som hanterar personuppgifter. Kartläggningen visar att GDPR-kraven i huvudsak är delvis uppfyllda. Tekniska skydd finns till viss del, men brister i loggning, spårbarhet och incidentrapportering gör att kraven inte uppnås fullt ut.

Även CER-direktivet är relevant för verksamheten. Här är kraven till största delen delvis uppfyllda. Grundläggande skyddsåtgärder och redundans finns, men det saknas tillräcklig dokumentation, strukturerad riskuppföljning och tydlig säkerhetsstyrning.

När det gäller Ellagen bedöms kraven också delvis uppfyllda. Det finns tekniska lösningar för driftsäkerhet, men beroendet av IT- och OT-system gör att brister inom cybersäkerhet och incidenthantering kan påverka efterlevnaden.

Samlad bedömning av kravuppfyllelse

- Uppfyllda krav: Få (inklusive ett krav inom NIS2)
- Delvis uppfyllda krav: Majoriteten
- Ej uppfyllda krav: Framför allt inom loggning, incidentrapportering, riskhantering och leverantörsstyrning

Sammanfattning av riskanalys

Det man kan säga är att den nuvarande situationen om hur det saknas tillräcklig loggning, riskhantering, incidentrapportering och leverantörsstyrning. det är oacceptabelt att inte ha dom bitarna i ett så stort företag är för att det kan leda till stora konsekvenser i framtiden så det är något som måste lösas så snart som man kan

Ett område vi var oroliga över är logghanteringen generellt. Eftersom mycket av verksamheten använder API:er och är kritisk infrastruktur vill vi säkerställa att alla loggning funkar som den ska, att de övervakas och att det finns åtgärder vid onormala händelser. Annars kan det ge hotaktörer chansen att öka sina behörigheter eller att intrång inte märkas.

En annan sak som ni måste skaffa så snart som möjligt är riskhantering för att utan den biten så kommer man inte hitta eller tänka på nya potentiella hot som kommer upp efter man gör förändringar, uppdateringar, nya funktioner, etc. Så det är en annan kritisk aspekt som måste bli framtagen.

Driftcentralen är också en del av verksamheten vi vill säkra upp mer. Eftersom det bara finns en driftcentral blir den en svag punkt som kan stoppa hela verksamheten, vill vi öka redundansen och säkerställa att centralen hanterar ett brett spektrum av incidenter som till exempel strömavbrott, cyberhot eller trasigt maskineri.

Mitigeringsstrategier och rekommenderade åtgärder

Det behöver införas mer loggning som kontrolleras regelbundet. Även backuper på loggarna. Loggarna ska vara dolda för utomstående, och ska vara låsta för ändringar.

Vid incidenter behöver kritisk personal vara tillgänglig för att hantera eventuella hot och driftproblem. Inventera personalen i ett tidigt skede för att fastställa roller.

Återkommande utbildning hos personalen att upptäcka spoofing och phishing för att undvika vanligt förekommande intrångsvägar. På en teknisk nivå kan man behöva scanna och logga inkommande och utgående trafik. Man bör även göra oregelbundna tester så att man kan se vilka personer som måste få ytterligare träning

Utbilda personalen att följa de regelverk som finns och ge inte behörigheter till individer som inte ska ha det. Om verksamheten täpper till hålen som gör att vissa regelverk inte är helt uppfyllda så är det många problem som kan åtgärdas. Regelverken är väldigt tydliga och lägger en bra grund för säkerheten.

Den enklaste och största åtgärden är utbildning i hela processen ända upp på ledningsnivå. Det hjälper personalen att själva upptäcka hot och inte falla för spoofing och phishing. Det i sin tur kommer underlätta för teknikerna som inte behöver oroa sig lika mycket för att någon på företaget utsätts.

Plan för uppföljning och förbättring

För att säkerställa att åtgärderna får avsedd effekt etableras en kontinuerlig uppföljningsprocess. Den bygger på mätning, utvärdering och förbättring enligt principerna i ett systematiskt säkerhetsarbete.

Kontinuerlig övervakning och mätning sker genom månatlig granskning av incidenter, loggar och sårbarhetsskanningar. Genom definierade KPI:er, såsom patch compliance, antal avvikelser och åtgärdstid, följs säkerhetsnivån upp och förbättringsbehov identifieras löpande.

Regelbundna revisioner genomförs för att säkerställa att organisationen följer fastställda policy och rutiner.

Arbetet kompletteras med löpande förbättringar där identifierade brister dokumenteras i en åtgärdsplan med tydligt ansvar och tidsramar. Erfarenheter från incidenter och övningar används för att uppdatera processer, och utbildningsinsatser justeras utifrån resultat från tester och analyser för att stärka säkerhetskulturen.

Rapportering och styrning sker genom regelbundna uppdateringar till ledning och relevanta intressenter, där prioriteringar anpassas efter förändringar i riskbild, verksamhetens behov och framväxande hot.

Reflektioner och Lärdomar

Namn: Jonas Beijbom
Roll: Riskanalys Ledare, lite kvalitetssäkringsansvarig
Eget bidrag: Kollat lite i regelverken. Ansvarade för systemkarta och styrde riskworkshopen. Försökt att tänka i metod vid riskanalyser. Identifierat hot och hur de kan åtgärdas. Skrivit i slutrapporten. Har försökt att dubbelkolla information.
Lärdomar: Det finns många regelverk som det är bra att ha koll på men också att det har många överlapp. Vid riskworkshops är det viktigt att man har allt underlag med sig så att man lättare kan göra riskbedömningar. Vi har haft bokade tider som alla har kommit till vilket har gjort att projektet alltid rullat framåt, det är alltså viktigt men en bra struktur och kommunikation på arbetet.
Förbättringsförslag: Jag skulle ha gjort ett bättre arbete på att kartlägga all information från översikten för att förenkla vårt arbete med riskworkshopen. Då hade det gått smidigare med att veta vilka åtgärder som redan var på plats och vad som akut saknades.

Namn: Daniel Wagenius
Roll: Dokumentationsansvarig
Eget bidrag: Skapat, underhållit och formaterat dokument. Skapat presentation. Har varit med i research och dokumenterat.
Lärdomar: Regelverken hänger ihop med varandra en hel del. Många regelverk gäller för företag som jobbar med kritisk infrastruktur. Viktigt att gå in i detalj när man säkrar upp. Har sett hur mycket jobb det är att ta fram en sån här stor rapport och få den att se bra ut, vara sammanhängande, och visa vem i gruppen som har gjort vad.
Förbättringsförslag: Jag borde ha tagit fram mallar i god tid för att ha samma eller i alla fall liknande utseende på alla dokument och det vi gjort.

Namn: Samuel
Roll: Projektledare, Riskanalys ledare,
Eget bidrag: Hjälpte till bygga bygga ihop systemkartan med jonas, Har även hjälpt till i nästan alla olika delar av uppgiften gällande brainstorming om risker och hot, reglering sök, dokumenterar etc,
Lärdomar: Jag har lärt mig att Jonas är mer passande som projekt ledare, han styrde upp det bättre än vad jag kunde göra, jag har dock även lärt mig att många saker hänger ihop på olika sätt även om dom kanske ser ut att vara orelaterade från ett perspektiv, en annan sak är att när man är flera personer så får man flera olika perspektiv om samma område vilket betyder att man gör ett mycket bättre jobb för att alla har sina olika tankar och insikter om vad olika risker eller problem kan vara
Förbättringsförslag: Om jag skulle bli en projektledare igen måste jag vara bättre på att ta initiativet med vad som ska göras härnäst.

Namn: Abdihakim
Roll: Teknisk säkerhetsanalytiker
Eget bidrag: jag har arbetat med teknisk analys, riskbedömning och tagit fram rekommenderade säkerhetsåtgärder. Jag har också försökt hjälpa mina gruppkamrater när det behövts för att förstå flera delar av projektet och inte enbart fokusera på min egen tekniska roll. Har även varit delaktig i diskussioner kring hot, loggning och säkerhetslösningar, samt tagit del av regelverken för att säkerställa att våra analyser och rekommendationer följer relevanta krav.
Lärdomar: Jag har lärt mig hur viktigt det är att koppla tekniska risker till verksamhetens behov och att tydliga processer gör riskarbetet mycket enklare. Jag har också fått en bättre förståelse för hur teknisk analys behöver kombineras med praktiska åtgärder som faktiskt går att genomföra. Samarbetet i gruppen har också visat hur mycket bättre resultat man får när flera perspektiv möts.
Förbättringar: Till nästa projekt vill jag bli bättre på att samla och strukturera information tidigt, eftersom det hade underlättat riskanalysen. jag ser också att vi skulle vinna mycket på att automatisera delar av arbetet, till exempel sårbarhetskontroller och loggranskning. det skulle göra processen snabbare och minska mängden manuellt arbete.

Namn: Erik Alduaifi
Roll: Regelverksanalytiker
Eget bidrag: Jag har jobbat med att ta reda på vilka regelverk som gäller för verksamheten, till exempel NIS2, GDPR och CER. Jag har hjälpt till att koppla reglerna till de risker vi hittade och sett till att våra förslag följer kraven. Jag har också varit med i diskussioner om incidenthantering, loggning och dokumentation samt stöttat gruppen när det gällt frågor om regelverk.
Lärdomar: Jag har lärt mig att många regelverk hänger ihop och att samma brist kan påverka flera lagar samtidigt.Jag håller dock med min kollega Jonas om att det finns många regelverk som är viktiga att ha koll på, men också att många av dem överlappar varandra. Jag har också lärt mig hur viktigt det är att tänka på regelverken tidigt i arbetet med riskanalys. Arbetet i gruppen har visat att man får ett bättre resultat när man är flera och kan se problem ur olika perspektiv.
Förbättringar: Till nästa projekt hade jag velat skapa en ännu tydligare överblick över regelverken tidigare i arbetet. Det hade gjort det lättare att snabbare se vilka krav som redan var uppfyllda och vad som saknades samt hade underlättat samarbetet i gruppen.