Rapport till Lyrestads Gjuteri AB

Informationssäkerhetsstudie genomförd: 2021-04-29

Författare:

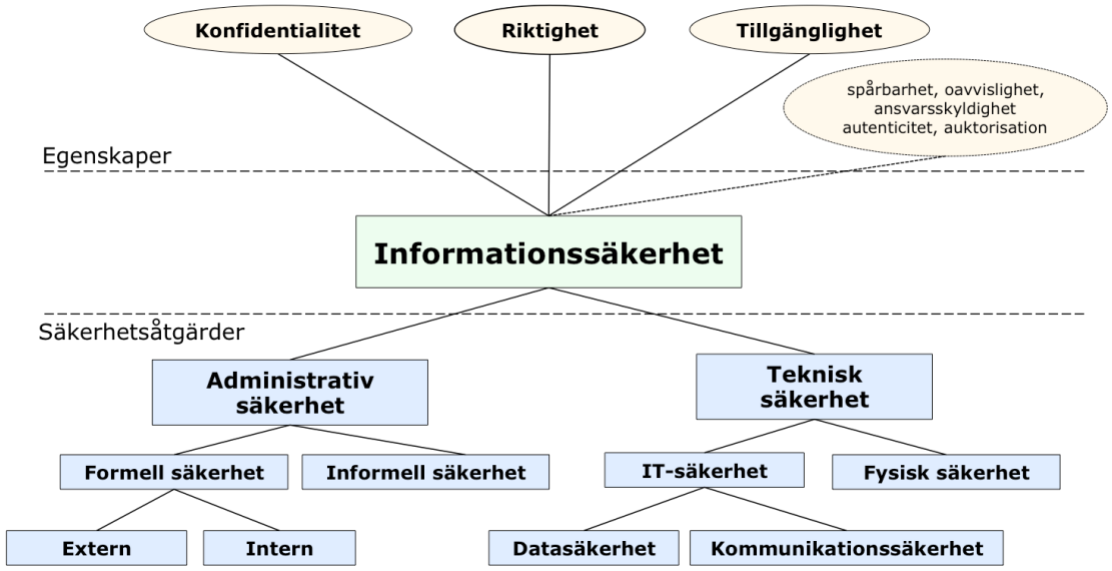
Anton Karlsson, c20antka@student.his.se
Lucas Hedlund, a20luche@student.his.se

BAKGRUND

Denna rapporten gjordes i samband med en gruppuppgift för Högskolan i Skövde, företaget som valdes ut var Lyrestads Gjuteri för att vi hade en nära kontakt på företaget. Vi fokuserade mycket på fysisk säkerhet på grund utav riskerna med gjuteri branschen samt deras säkerhet på nätverk och server där de lagrar sin data. Vi genomförde rapporten genom att åka till Lyrestad och gjorde en intervju på plats för att få en bra insikt i hur lokaler och område såg ut samt fabrik. Vi gjorde rapporten på plats för att det är mycket fysisk säkerhet som är hög prioritet inom gjuteribranschen, även om de blir mer och mer tekniska samt behandlar mer data och 3D CAD modeller som behöver lagras säkert.

ÖVERGRIPANDE NULÄGE

Säkerheten idag är väldigt medelmåttig på företaget, den externa fysiska säkerheten är låg. Administrativa säkerheten har ingen spårbarhet och policy för datahantering finns inte. Till exempel känsliga data som inte ska lämna servern kan tas med hem för jobb hemifrån. Tekniska säkerheten är relativt bra eftersom server och mappar är lösenordskyddade och sannolikt krypterade men kontakten kunde inte svara helt säkert på det. För åtkomst till den utomstående servern (molnlagringen) så behövdes VPN för åtkomst samt autentisering, så i det avseende så var säkerheten relativt bra (kunde varit bättre med tvåfaktors autentisering). Informationssäkerheten var definitivt ingen prioritet på företaget men var något de var intresserade utav att förbättra, att informationssäkerheten var relativt låg är på grund utav bristande kunskap inom området. Därför var de glada över analysen och förbättringsförslag samt var intresserade utav att utforma en informationssäkerhetspolicy för att utveckla standarder.



Figur 1 - Informationssäkerhetsmodellen

ADMINISTRATIV SÄKERHET

FORMELL SÄKERHET

Extern

Företaget följer inga utomstående policys eller standarder för informationssäkerhet, följer inte 27001 ISO.

Följer dock ISO standarder för miljö och kvalité (ISO 14001 & 9001).

Intern

Företaget har ingen egenutformad informationssäkerhetspolicy i dagsläget.

INFORMELL SÄKERHET

Vissa hemliga prototypers information finns endast på papper eller i huvudet på chefen, som då är väldigt informellt.

TEKNISK SÄKERHET

IT-SÄKERHET

Datasäkerhet

En äldre dator kör ett gammalt ej längre stött operativsystem som då är en säkerhetsrisk.

Datan som är lagrad på servern i det lokala nätverket är (förmodligen) krypterad och lösenordsskyddad.

För att komma åt datan som ligger lagrad off-site krävs VPN med rätt login och sedan rätt lösenord för filåtkomst.

Kommunikationssäkerhet

Deras företagsdomän via loopia har kryptering för email.

FYSISK SÄKERHET

Byggnaden är brandklassad, har dock inga säkerhetsdörrar eller passerkontroll.

Cupola är anställda för att sköta brandöverkoll, brandskydd (sker 3 gånger per år), kontroll utomhus för att överskåda brandrisk (en gång i veckan).

Finns flertalet pulversläckare på plats, krav på klädsel i fabrik.

Brandlarm, dock inga automatiska åtgärder kopplade till larmet (eftersom gjuteri inte kan ta emot vanlig brandbearbetning, vatten på gjutet järn i produktion kan orsaka explosioner och vattnet kan bränna personal).

Utbildning brandutrymmning.

FÖRBÄTTRINGSFÖRSLAG

En bra början för förbättrning är att utforma en säkerhetspolicy och börja vara mer medvetna om informationssäkerhet, i dagsläget har det helt enkelt fallit mellan stolarna. Då de har utformade policies för andra delar i förtaget kan det enkelt utformas en här också med rätta riktlinjer.

För att lösa informationssäkerhetspolicyn erbjöd vi information som kan hjälpa till att strukturera en policy (en sammanställning utav bra punkter från Pfleeger, 2015).

En viktig förbättring är att byta ut datorn med windows 7 operativsystem eftersom det OS inte längre uppdateras och är en säkerhetsrisk i nätverket. Dock kommer denna att bytas ut snart eftersom de har beställt ett helt nytt system som ska implementeras i företaget där alla datorer ska köra Windows 10 PRO för att fungera med det nya systemet.

Priset för systemet angavs inte.

Mejlen som skickas ska gå under kryptering men generellt så är e-mejlens säkerhet obefintlig så därför bör personalen utbildas i att känslig information ej ska skickas via e-mejll. I dagsläget finns många användbara program och appar som använder sig utav krypterade chattar som då kan användas istället (kräver dock att båda parter är villiga att använda det).

Företaget bör skaffa sig någon typ av inbrottssäker dörr och ta kontroll över vilka som kommer ut och in på kontoret, i dagsläget är det en väldigt vanlig dörr som lätt kan brytas upp och då har du snabbt och enkelt fullt inträde till kontor där dator och lagring finns. De har även talat om att sätta upp kameror för att se aktivitet utanför då de har haft problem med stölder utav järn förut som kan finnas på gården.

Säkerhetsdörr kostar mellan 10 och 20 tusen beroende på säkerhetsklass, eftersom det gäller ett företag hade en säkerhetsklassning så som RC4 rekommenderats.

För kameraövervakning rekommenderar vi en wifi-baserad rotationskamera för hörnet utav byggnaden så övervakning för framsida (ingång) och samt gårdsplanen på sidan kan övervakas utav en och samma kamera med 360 graders täckning, en smidig och enkel installation och styrning med hjälp av en app. Kostnaden för en bra kamera som klarar av detta i utomhus miljö kostar mellan 20 och 30 tusen kronor.

Utbilda sig i informationssäkerhet med hjälp av konsulter/kurser är ett bra alternativ i alla fall för en person som får informationssäkerhets som deras område på företaget. Finns kurser som täcker ISO 27001 standarden, priser kan variera beroende på längd och omfång (uppskattat pris från 5000kr och uppåt).

ADMINISTRATIV SÄKERHET

FORMELL SÄKERHET

Extern

Företaget följer inga policys/standarder som berör deras informationssäkerhet, exempelvis ISO 27001 men eftersom de följer både ISO 9001 och ISO 14001 så är det inga större problem att införskaffa då 27001 är nära besläktad med 9001 och 14001 vilket gör att den kan enkelt integreras med övriga standarder.

Intern

Identifiera och analysera verksamhetens informationstillgångar och göra en riskanalys.

INFORMELL SÄKERHET

Månadsvis gå igenom eventuella säkerhetsaspekter med de anställda.

TEKNISK SÄKERHET

IT-SÄKERHET

Datasäkerhet

Operativsystemet som finns i produktion ska bytas ut till ett nyare vilket är viktigt då en svag punkt kan utnyttjas och komma åt verksamhetens tillgångar. Ett och samma operativsystem som alltid är uppdaterat för att skydda sig från nya virus och liknande.

Brist på spårbarhet, kan endast se om en ändring eller borttagning av fil sker. Här kan en ökad spårbarhet öka säkerheten genom att se vem som gör det. Samtidigt är övervakning av loggar kanske inte nödvändigt baserat på vad verksamheten gör.

Kommunikationssäkerhet

Se över vilken typ av brandvägg som används och om den är alltid är aktiverad.

FYSISK SÄKERHET

Säkra utrymmen så att obehöriga inte får tillträde genom exempelvis säkerhetsdörr.

Lokala skalskydd, används valv eller kassaskåp där känslig information förvaras?

Eftersom företaget inte har en receptionist hur sker in- och utpassering, hur tas externa besökare emot, hur bekräftas besöken?
Alternativ kan vara att skaffa en loggbok.

Utbilda personalen i brand och olyckor om hur de ska agera vid brand.

DISKUSSION

Deras säkerhet överlag var relativt låg, den fysiska säkerheten samt den tekniska säkerheten behöver trappas upp. Server-säkerheten är ändå ganska hög tack vare deras IT konsult, men de behöver bygga upp en plan för deras säkerhetsarbete, samt ta fram vilken information som är viktigast att skydda. En bra början är att säkerställa en säkerhetspolicy som nämnts ovan, som de själva behöver jobba med regelbundet eftersom säkerhetskraven ständigt ändras. Försöka skapa ett intresse bland de anställda om säkerheten överlag på fabriken genom att följa upp hur de ser på den dagliga produktionen, evenutella risker samtom det är något som kan förbättras.

En bra början är den fysiska säkerheten för att hålla ute ej välkomna personer med bra dörr och lås samt kameraövervakning om inbrott eller att någon smiter in under dagtid. På så sätt kan företaget få en bra överblick över vad som sker vid in- och utpassering såväl dagtid men även om det skulle ske något plötsligt då ingen personal finns där. För att utöka säkerheten vid inpassering kan en loggbok finnas till hands vid ingången så att alla som besöker fabriken skriver in sitt namn och eventuellt företag de representerar samt tid för deras besök. Det ger företaget kontroll över vilka som besöker företaget och minskar risken att obehöriga får tillträde.

Något som är värt att påpekas är att organisationen bör arbeta med sin säkerhetsplan utifrån deras storlek och användning. Det vill säga att säkerheten ska vara anpassad för deras behov och risker och skapa ett mervärde. Ett för stort fokus på säkerheten kan kosta mer än det smakar. Organisationen ska se till att deras säkerhet skapar en nytta så det på ett effektivt sätt skapar ett värde. Därav är analysfasen viktig för att se över organisationens behov för att skapa en strukturerad och systematisk arbete.

Vi vill även rikta ett stort tack till Lyrestads gjuteri för samarbetet och önskar dem lycka till med sin säkerhet i framtiden!

REFERENSER

Creator (2021) *ISO 27001 [Online].* Available at http://www.creator.nu/informationssakerhet-enligt-iso-27001 *(Accessed 6 Maj)*

Dustin (2021) *Axis P5655-E 50 Hz* [Online]. Available at *https://www.dustin.se/product/5011174541/p5655-e-50-hz?ssel=false&gclid=Cj0KCQjwytOEBhD5ARIsANnRjVhcyrzQ2Ucd9djmKbLF7MmkGnRUhdZptDVxtmDU6TdACvIhimDViZEaAkPzEALw_wcB* (Accessed: 6 Maj)

St.GEORGE (2021) *Säkerhetsdörr I standardutförande St George [Online].* Available at https://www.stgeorge.se/sakerhetsdorr-st-george-klass-3.html?utm_source=kelkoo&utm_medium=affiliate&utm_campaign=uk&amss=j3a&from=kelkoo&gclid=Cj0KCQjwytOEBhD5ARIsANnRjVji79FQNNP0tVCLsRLO-tAGywqsPzFBPupEEWFWcPgrX0Pj1MvmzNEaAg1zEALw_wcB