Informationssäkerhet

Henrik Jansson

DevOps Engineer, 2023

Handledare Cihan Viviera
Datum 14 juni. 2024

Inlämningsuppgift har genomförts inom ramen för yrkeshögskolestudier vid Lernia.

Innehåll

1 Inledning

Henidia Graphics, är ett av de världsledande företaget inom grafikteknik. Företaget hanterar och lagrar känslig information om sina kunder, anställda samt konfidentiell företagsinformation om sina produkter etcetera. På grund av storleken och med snabb tillväxt har behovet av att granska och förbättra företagets informationssäkerhetspolicy ökat. Ledningen har insett vikten av att skydda företagets information från både interna och externa hot och söker därför en uppdaterad informationssäkerhetspolicy.

1.1 Syfte och mål med säkerhetspolicy

Syftet och målet är att skapa en informationssäkerhetspolicy säkerställa integriteten och konfidentialiteten och arbeta för en säker miljö.

En säkerhetspolicy omfattas av områden ska hanteras av de anställda inom organisationen. Detta omfattas till exempel av arbete med, skydda känslig information, säkerställa systemets integritet, riskhantering, incidenthantering, efterlevnad

Händelser och incidenter ska dokumenteras kontinuerlig och utbildning av personal bör vara av högsta prioritet för att minska risker hot. Att öka medvetenheten om risker och dess påverkan är i dagens samhälle viktigt i takt med den utveckling som sker för att säkerställa att alla är medvetna om potentiell påverkan av en katastrof.

2 Vad informationssäkerhet är

- Definition: Informationssäkerhet avser skyddet av information och informationssystem mot obehörig åtkomst, användning, avslöjande, störning, modifiering eller förstörelse för att säkerställa konfidentialitet, integritet och tillgänglighet.

- Utbildning: Alla anställda ska genomgå grundläggande utbildning i informationssäkerhet vid anställningens början och därefter regelbundet.

- Medvetenhet: Informationskampanjer och påminnelser om informationssäkerhet ska regelbundet distribueras till alla anställda.

3 Riskanalysrapport

Risk typ	Externa hot	Interna hot
Cyberattacker	Högt: Angripare kan utnyttja sårbarheter i systemet för att stjäla data eller orsaka skada.	Måttligt: Anställda kan oavsiktligt eller avsiktligt orsaka säkerhetsproblem.
Dataintrång	Måttligt: Obehöriga kan få tillgång till känslig information.	Högt: Anställda kan oavsiktligt läcka information eller otillåtet dela den.
Åtkomst och behörigheter	Måttligt: Felaktig hantering av användarbehörigheter kan leda till oavsiktlig dataåtkomst.	Måttligt: Felaktig hantering av behörigheter kan leda till oavsiktlig dataåtkomst.
Efterlevnadsrisker	Lågt: Brott mot regler och standarder kan leda till böter eller rättsliga konsekvenser.	Måttligt: Felaktig efterlevnad av regler kan leda till sanktioner.

4 Informationssäkerhetspolicy

Henidia Graphics AB

4.1 Principer för säkerhetsarbetet

- Riskidentifiering: Regelbundna riskbedömningar ska genomföras för att identifiera potentiella hot och sårbarheter.
- Riskbedömning: Alla identifierade risker ska bedömas utifrån sannolikhet och potentiell påverkan. Dokumentation och granskning bör ske regelbundet.
- Riskprioritering: Risker ska prioriteras baserat på deras potentiella påverkan och sannolikhet. Riskerna bör estimeras beroende på hotbilden.
- Chefer på högsta nivå har ett ansvar för att medarbetare har tillräcklig kunskap kring riktlinjer och policys.
- Medarbetarna på alla nivåer har ett ansvar för att följa det interna säkerhetsregelverket,

genomgå utbildning, vara uppmärksamma och rapportera brister och incidenter omgående.

- Säkerhetsnivån och bestämmelser kring detta ska framgå klart och tydligt.

4.2 Analysera och granska säkerhetsincidenter

Incidenthantering:
Säkerhetsincidenter ska rapporteras till IT-avdelningen och dokumenteras i ett incidenthanteringssystem och ska helst ske med omedelbar verkan.

Incidentanalys:
Genomföra grundliga analyser av incidenter för att identifiera svagheter i systemet/systemen

Incidentgranskning:
Regelbundna granskningar av incidentrapporter ska genomföras för att identifiera mönster. Lärdomar ska göra individen medveten om förbättringar som kan ske

5 Hotbild & potentiell påverkan

- Malware, Phishing, Ransomware, DDoS-attacker, Insider hot
- Dataförlust, Driftstopp, Ekonomiska förluster, Skadat rykte
- Informera och utbilda anställda.
- Hur de kan skydda sig själva och företaget
- Sanktioner

6 Principer och procedurer för arbetet med säkerhetspolicy

6.1 Konfidentalitet
Konfidentialitet innebär att information endast är tillgänglig för de som har behörighet att se den. Det skyddar känslig information från att bli åtkommen av obehöriga parter.

6.2 Integritet
Integritet säkerställer att informationen är korrekt och oförändrad. Det innebär att data inte ska kunna manipuleras eller förstöras av obehöriga parter.

6.3 Tillgänglighet
Tillgänglighet innebär att information och system är tillgängliga för behöriga användare när de behövs. Det säkerställer att viktiga tjänster och data kan nås utan avbrott vid behov.

6.4 Policyutveckling:
Säkerhetspolicyer ska utvecklas i samarbete med berörda avdelningar och baseras på riskbedömningar och branschstandarder.

6.5 Godkännande och publicering:

Alla säkerhetspolicyer ska godkännas av företagsledningen och kommuniceras till alla anställda.

6.6 Implementering:

Säkerhetspolicyer och procedurer ska implementeras i en riktlinje som är väldigt tydlig och klargöra ansvarsområden för att säkerställa rätt efterlevnad.

6.7 Granskning och Uppdatering:

Säkerhetspolicyer och procedurer ska regelbundet granskas och uppdateras för att anpassas till förändrade hot och verksamhetsbehov.

7 Nulägesanalys och Omvärldsbevakning

7.1 Aktuella trender och hot inom informationssäkerhet

Trenden med ransomware attacker är nu och sedan tidigare den mest vanligaste och det påtagliga hotet inom informationssäkerhet. Hackaren angriper med hjälp krypterad mjukvara vilket leder till att lösenord krävs för att återställa tillgången till systemen. Utpressning av pengar är vanligt i denna metod. Samarbeten, analyser, utbildning och olika säkerhetsrapporteringar är en stor del av arbetet för att proaktivt identifiera och hantera potentiella risker i och med detta krävs en bra integrationen av omvärldsbevakning.

7.2 Relevanta standarder:

27001 SS-EN OSCA/IEC är en standard som bör tillämpas, och det spelar ingen roll i vilken omfattning och storlek på organisationen. Denna **standard** ska **alltid** följas.
ISO 27000, är serien för informationssäkerhet och omfattar cybersäkerhet och dataskydd.

8 Roll- och Ansvarsbeskrivning

8.1 Ledningens ansvar och betydelse

Det övergripande ansvaret för informationssäkerhet ligger hos ledningen. Är ledningen engagerad och införstådd med nyttan av säkerheten bidrar detta till en högre säkerhetsmedvetenhet inom organisationen och de anställda.

8.2 Samverkan mellan olika roller

För att kontinuerligt sträva mot en säkrare miljö krävs det att alla har förståelse för hotbild och risker som finns. Att inom organisationer använda sig av CISO, vilket är ett stöd i uppgiften med att utveckla och samordna säkerhetsarbetet i organisationen.

Sammanfattningsvis är hela organisationen ansvarig för löpande arbetet. Genom workshops och veckobrev kan vi öka medvetenheten och samspela genom alla de olika avdelningar som organisationen består av.

9 GDPR-analys

9.1 Påverkan av GDPR på informationssäkerheten

Att lagra och hantera data på ett felaktigt sätt kan få stora konsekvenser som kan resultera i enorma ekonomiska förluster. Den globala handeln bidrar till hårdare och höjda informationssäkerhetsstandarder.

9.2 Åtgärder för att säkerställa GDPR-efterlevnad

Använda sig av krypteringar, åtkomstkontroller och regelbundet granska säkerheten. Organisationen bör ha en färdig plan för hantering av incidenter och rapportering. Detta ökar chansen att skadorna vid en potentiell händelse blir lägre.