Säkerhetsåtgärder i informationssystem

bedömningsverktyg

Förord

Med införandet av NIS2-direktivet ökar kraven på hantering av säkerhetsåtgärder i informationssystem för organisationer. För att säkerställa efterlevnad och stärka skyddet mot cyberhot behövs en tydlig struktur för riskbedömning och säkerhetsåtgärder. Vi på Gridheart har tagit fram ett bedömningsverktyg, som ni kan använda gör att utvärdera säkerhetsnivån, identifiera brister och implementera åtgärder i enlighet med NIS2.

Detta bedömningsverktyg är en tolkning och summering av den fulla versionen från MSB. Se källa; MSB (2023)

2. Grundläggande förutsättningar
2.1 Ansvar

Syfte

Det behöver vara tydligt i organisationen vem som ska se till att tillräckliga säkerhetsåtgärder införs i ett informationssystem, och att det finns resurser för att anpassa säkerhetsåtgärderna när organisationens behov eller förhållanden i omvärlden förändras.

Krav

Organisationen ska se till att...

1. varje informationssystem har en systemägare.
2. systemägaren ansvarar för att införa, förvalta, följa upp och utvärdera säkerhetsåtgärder
3. systemägaren har resurser för att införa och förvalta tillräckliga säkerhetsåtgärder i informationssystemen.

2.2 Omvärldsbevakning

Syfte

Organisationen behöver bedriva omvärldsbevakning för att kunna identifiera och hantera hot mot och sårbarheter i organisationens informationssystem.

Krav

Organisationen ska se till att bedriva omvärldsbevakning för att...

1. identifiera potentiella hot mot sina informationssystem
2. identifiera potentiella sårbarheter i sina informationssystem
3. hitta stöd för hanteringen av hot mot och sårbarheter i sina informationssystem.

Mening:
En organisation behöver följa utvecklingen på informations- och cybersäkerhetsområdet för att hålla sig uppdaterad om nya hot, sårbarheter och teknisk utveckling.
Organisationen behöver välja relevanta källor för sin omvärldsbevakning, exempelvis; IMY, MSB, PTS, FMV, ENISA, NIST, CISA, CIS, OWASP.

2.3. Riskbedömning

Syfte

Organisationen behöver identifiera, analysera och värdera risker för att kunna vidta ändamålsenliga och proportionerliga säkerhetsåtgärder för sina informationssystem.

Krav

Organisationen ska...

1. se till att det finns ett arbetssätt för att identifiera, analysera och värdera risker
2. genomföra riskbedömning av produktionsmiljön i sin helhet
3. genomföra riskbedömning av enskilda informationssystem var för sig eller samlat för informationssystem i produktionsmiljön med liknande funktion, uppbyggnad och användningsområde

Organisationen bör...

1. se till att det även genomförs en riskbedömning för organisationens;
    a. utvecklingsmiljö
    b. testmiljö
    c. utbildningsmiljö
2. ge systemägaren i uppgift att säkerställa att riskbedömningen genomförs för de informationssystem som systemägaren ansvarar för

Riskbedömning

Riskbedömning handlar om att besvara frågorna: ”Vad kan hända?”, ”Varför kan det hända?”, ”Vad blir konsekvenserna?” och ”Hur sannolikt är det att det inträffar?”. Underlaget för att identifiera hot och sårbarheter kommer bland annat från omvärldsbevakning. Konsekvenser kan vara ekonomiska förluster, merarbete, hälsoproblem eller skadat förtroende.

2.4 Dokumentation av IT-miljön

Syfte

Organisationen behöver dokumentera sin it-miljö, dess olika delar, ingående informationssystem, beroenden samt den hård- och mjukvara som används i it-miljön för att kunna bedriva säker drift och förvaltning.

Krav

Organisationen ska för samtliga informationssystem ha uppdaterad dokumentation om...

1. vilken hård- och mjukvara som används i varje informationssystem.
2. vilka beroenden som finns till andra interna informationssystem
3. vilka beroenden som finns till informationssystem hos externa aktörer
4. om informationssystemet behandlar information i behov av utökat skydd
5. om informationssystemet är särskilt viktigt för organisationens möjlighet att bedriva sin verksamhet.

Organisationen bör...

1. använda tekniskt stöd för att säkerställa att dokumentation om exempelvis informationssystemets hård- och mjukvara samt beroenden är uppdaterad
2. beskriva beroenden mellan informationssystem i en systemkarta eller motsvarande
3. använda informationsklassning för att identifiera vilka informationssystem som behandlar information i behov av utökat skydd.

3. Utveckling, anskaffning och utkontraktering

3.1 Kravställning

Syfte

Organisationer behöver, inför utveckling, anskaffning av informationssystem eller utkontraktering av informationsbehandling kunna identifiera vilka krav på säkerhetsåtgärder som ska kunna ge information och informationssystem tillräckligt skydd.

Krav

Organisationen ska...

1. vid utveckling, anskaffning eller utkontraktering av informationssystem, identifiera krav på säkerhet avseende;

a. uppdelning i nätverkssegment	j. säkerhetsloggning och tillhörande analys
b. filtrering av nätverkstrafik	k. övervakning av nätverkstrafik
c. behörigheter, digitala identiteter och autentisering	l. övervakning av informationssystem inklusive säkerhetsfunktioner
d. kryptering	m. skydd mot skadlig kod
e. säkerhetskonfigurering	n. skydd av utrustning
f. säkerhetstester och granskningar	o. redundans och återställning
g. ändringshantering, uppgradering och uppdatering	p. kontinuitet under fredstida krissituation samt inför och vid höjd beredskap
h. robust och korrekt tid	q. arkivering
i. säkerhetskopiering	r. avveckling

2. dokumentera vilka säkerhetsåtgärder som valts för att möta respektive krav.

Organisationen bör...

1. vid val av säkerhetsåtgärder kombinera organisatoriska, administrativa, fysiska och tekniska åtgärder

2. gruppera beslutade säkerhetsåtgärder i olika skyddsnivåer, som bör motsvara de olika konsekvensnivåerna som används vid informationsklassningen.

3. vid anskaffning av informationssystem överväga att välja produkter som är certifierade genom tredjepartsgranskning mot etablerad standard.

3.2 Kontroller

Syfte

För att kunna bedriva säker drift och förvaltning behöver organisationen, innan driftsättning och inför förändringar som kan påverka säkerheten i informationssystemen, kontrollera att valda säkerhetsåtgärder är införda och ger tillräckligt skydd.

Krav

Organisationen ska, innan drift sättning och inför förändring som kan påverka säkerheten i informationssystemen. Detta genom...

1. säkerhetsstester och granskning kontrollera att valda säkerhetsåtgärder är tillräckliga för att möta identifierade krav på säkerhet.
2. att verifiera att det finns nödvändig dokumentation för drift och förvaltning.
3. att genomföra riskbedömning och hantera brister som identifierats genom säkerhetstester och granskning samt vid verifiering av dokumentationen.

Organisationen bör se till att dokumentation för drift och förvaltning av informationssystem omfattar...

1. arkitektur, ingående komponenter, konfiguration, dataflöden och övrig relevant systeminformation
2. Vem som är systemägare
3. om och till vilken extern aktör utkontraktering har skett.

Genomför kontroller innan driftsättning:

Kontroller innan driftsättning:

Innan ny hårdvara eller mjukvara driftsätts bör kontroller göras för att upptäcka säkerhetsbrister. Detta kan göras genom säkerhetstester, granskning eller verifiering av dokumentation, t.ex. genom att testa uppdateringar i testmiljö innan de installeras. Nyinköpt hård- och mjukvara ska kontrolleras för att säkerställa att de är uppdaterade. Organisationen bör ha fastställda arbetssätt för att genomföra dessa kontroller, och tester som påverkar IT-miljön bör utföras av kompetenta personer.

3.3 Utvecklings-, test- och utbildningsmiljöer

Syfte

För att skydda organisationens produktionsmiljö från incidenter som kan uppstå i organisationens utvecklings-, test- och utbildningsmiljöer behöver organisationen skilja produktionsmiljön från dessa miljöer.

Krav

Organisationen ska...

1. bedriva sitt arbete med utveckling och tester som kan påverka säkerheten i en it-miljö som är avskild från produktionsmiljön.
2. identifiera och hantera behovet av en utbildningsmiljö som är avskild från produktionsmiljön.

4.0 Drift och förvaltning
4.1 Nätverkssegment och filtrering

Syfte

För att förhindra spridning och konsekvenser av inträffade incidenter behöver organisationen dela upp sin it-miljö i olika nätverkssegment och filtrera trafiken så att endast nödvändiga dataflöden förekommer.

Krav

Organisationen ska...

1. placera informationssystem med olika funktioner i separata nätverkssegment i sin produktionsmiljö
2. filtrera nätverkstrafiken så att endast nödvändiga dataflöden förekommer mellan olika nätverkssegment.

Organisationen bör placera följande funktioner i separata nätverkssegment:

1. klienter för användare
2. klienter för administration
3. servrar
4. centrala systemsäkerhetsfunktioner i form av behörighetskontrollsystem, säkerhetsloggning, filtrering och liknande
5. centrala stödfunktioner i form av skrivare, scanner och liknande
6. trådlösa nätverk
7. gästnätverk
8. externt åtkomliga tjänster
9. informationssystem som sammankopplas med informationssystem hos extern aktör
10. industriella informations- och styrsystem
11. system som innehåller sårbarheter som inte kan hanteras.

Indelning i zoner

Arbetet med att dela in nätverket i olika segment underlättas om organisationen, lämpligen systemägaren för nätverket, dessförinnan har beskrivit designen i nätverket på övergripande nivå. Designen kan illustreras med hjälp av en zonmodell. De olika zonerna i en sådan modell kan skilja sig åt, exempelvis avseende användningsområde, skyddsbehov och möjlighet till extern kommunikation.

4.3 Autentisering

Syfte

För att skydda organisationens informationssystem mot obehörig åtkomst behöver organisationen ha interna regler för att skydda sina autentiseringsuppgifter och i vissa fall använda flerfaktorsautentisering.

Krav

Organisationen ska...

1. använda flerfaktorsautentisering vid...
    a. egen och inhyrd personals åtkomst till produktionsmiljön via externt nätverk
    b. systemadministrativ åtkomst till informationssystem
    c. åtkomst till informationssystem som behandlar information som bedömts ha behov av utökat skydd
2. ha interna regler för hantering av autentiseringsuppgifter med krav på
    a. längd och komplexitet
    b. när byte ska ske
    c. hur distribution ska ske
    d. hur autentiseringsuppgifterna ska skyddas.

Organisationen bör även använda tekniska system för att stödja efterlevnaden av reglerna avseende autentiseringsuppgifternas längd, komplexitet och byte.

4.4 Kryptering

Syfte

För att skydda organisationens information mot obehörig åtkomst och obehörig förändring, både vid överföring och lagring, behöver organisationen använda kryptering på ett sätt som motsvarar behoven.

Genom kryptering går det också att verifiera att den information som en avsändare skickat
är densamma som mottagaren tar emot (autenticitet avseende innehåll). Det går även att verifiera att meddelandet kommer från den avsändare som uppgivits (autenticitet avseende ursprung)

Krav

Organisationen ska...

1. identifiera och hantera behovet av kryptering för att skydda informationen mot
    a. obehörig **åtkomst** vid överföring och lagring
    b. obehörig **förändring** vid överföring och lagring
2. ha interna regler för kryptering med krav på
    a. hantering av krypteringsnycklar
    b. godkännande och förvaltning av krypteringslösningar
    c. val av krypteringsalgoritmer, krypteringsprotokoll och nyckellängder
3. använda Domain Name System Security Extensions (DNSSEC) för domännamn som är registrerade i domännamnssystemet (DNS)

Organisationen bör...

1. använda kryptering för att skydda
    a. säkerhetsloggar mot obehörig åtkomst och obehörig förändring
    b. autentiseringsuppgifter mot obehörig åtkomst och obehörig förändring
    c. information i behov av utökat skydd mot obehörig åtkomst och obehörig förändring vid överföring till informationssystem utanför organisationens kontroll.
2. införa möjlighet att verifiera organisationen som avsändare respektive mottagare av e-post.
3. identifiera behovet av att kryptera e-post på transportlagret.

4.5 Säkerhetskonfigruering

Syfte

För att skydda sin it-miljö mot obehörig åtkomst behöver organisationen byta ut förinställda autentiseringsuppgifter och konfigurera informationssystemen genom att endast tillåta nödvändiga systemfunktioner.

Krav

Organisationen ska, för att skydda informationssystem mot obehörig åtkomst...

1. **byta ut förinställda autentiseringsuppgifter**. Dessa kan vara kopplade till flera olika typer av identiteter (konton) för användare, informationssystem och systemadministratörer. Valet av nya autentiseringsuppgifter behöver göras enligt de interna reglerna för hantering av autentiseringsregler, så att behovet av längd och komplexitet tillgodoses
2. **stänga av, ta bort eller blockera system funktioner som inte behövs.** Uppdatera och uppgradera, koppla loss nätverkskablar, stäng ned onödig funktionalitet, ta bort för höga behörigheter och se till att anpassa konfigurationer.
3. i övrigt **anpassa konfigurationer för att uppnå avsedd säkerhet.**

4.6 Säkerhetstester och granskning

Syfte

För att identifiera och hantera sårbarheter i enskilda informationssystem och it-miljön i sin helhet, behöver organisationen kontrollera att informationssystemen är uppdaterade samt att valda säkerhetsåtgärder och säkerhetskonfigurationer är införda och tillräckliga.

Krav

Organisationen ska...

1. säkerställa att säkerhetstester och granskningar möjliggör identifiering av sårbarheter
2. ha interna regler för hur kontroll görs av att
    a. informationssystemen är uppdaterade
    b. valda säkerhetsåtgärder är införda på korrekt sätt
    c. **genomförda säkerhetskonfigurationer är tillräckliga**. Eftersom säkerhetstester och granskningar tar tid och resurser är det lämpligt att ta fram och använda ett standardiserat arbetssätt för säkerhetstester och granskningar som alltid utförs.

Organisationen bör även kombinera automatiserade säkerhetstester och manuella granskningar vid kontroll av säkerheten i informationssystemen.

Säkerhetstester syftar till att finna tekniska sårbarheter och genomförs i huvudsak genom sårbarhetsskanningar och intrångstester (penetrationstester eller pentest). Dessa tester genomförs för att identifiera sårbarheter och sätt som en angripare skulle kunna använda för att få åtkomst till organisationens informationssystem och it-miljö.

4.7 Ändringshantering, uppgradering och uppdatering

Syfte

För att genomföra ändringar i informationssystem utan att påverka säkerheten i it-miljön, behöver organisationen ha en strukturerad och spårbar ändringshantering.

Krav

Organisationen ska...

1. Säkerställa att ändringar i informationssystem görs på ett strukturerat och spårbart sätt.
2. Ha interna regler för ändringshantering, som inkluderar:
    a. *Kriterier för att godkänna hård- och mjukvara innan installation eller användning.*
    b. *identifiering och hantering av risker för incidenter och avvikelser vid förändringar i produktionsmiljön.*
    c. *Uppdatering av mjukvara till senaste version utan onödiga fördröjningar.*
    d. *Byta ut eller uppgradera hård- och mjukvara som inte längre stöds eller uppdateras av leverantören, utan onödiga fördröjningar.*
    e. *Hantering av risker om uppdatering eller uppgradering enligt c) och d) inte går att genomföra.*

Organisationen bör...

1. Snabbt införa säkerhetsuppdateringar.
2. Överväga att automatisera säkerhetsuppdateringar.
3. Förtydliga interna regler hur risker för incidenter och avvikelser vid förändringar i utvecklings-, test- och utbildningsmiljö ska hanteras.
4. Genomföra tester och ta fram en återställningsplan innan förändringar genomförs, för att undvika störningar.

4.8 Korrekt och spårbar tid

Syfte

För att kunna jämföra loggar mellan olika informationssystem och använda funktioner som ökar säkerheten vid kommunikation med andra, behöver organisationen använda den officiella svenska tiden från en pålitlig tidstjänst.

Krav

Organisationen ska använda korrekt och spårbar tid baserad på den svenska UTC-tillämpningen (UTC(SP)) i produktionsmiljön.

Organisationen bör...

1. Använda tidstjänsten Swedish Distributed Time Service via www.ntp.se.
2. Identifiera och hantera behovet av korrekt och spårbar tid även i utvecklings-, test- och utbildningsmiljöer.

4.9 Säkerhetskopiering

Syfte

För att kunna återskapa information som obehörigt eller av misstag har förstörts eller ändrats, behöver organisationen säkerhetskopiera sin information och skydda sina säkerhetskopior.

Krav

Organisationen ska...

1. Regelbundet säkerhetskopiera information för att kunna återställa förlorad eller skadad data.
2. Förvara säkerhetskopior åtskilda från produktionsmiljön och skydda dem mot skador, obehörig åtkomst och förändringar.

Organisationen bör...

1. Säkerhetskopiera viktig information en gång per dag för att stödja verksamheten.
2. Verifiera sin förmåga att återställa data från säkerhetskopior en gång per år eller vid större förändringar i produktionsmiljön.
3. Behandla programvara, konfiguration och information separat vid bedömning av säkerhetskopieringens omfattning och intervall.
4. Identifiera och hantera behovet av säkerhetskopiering och återställning i utvecklingsmiljöer.

4.10 Säkerhetsloggning

Syfte

För att i efterhand kunna upptäcka och hantera incidenter och avvikelser som kan påverka säkerheten i informationssystemen, behöver organisationen logga säkerhetsrelaterade
händelser.

Krav

Organisationen ska...

1. Säkerställa spårbarhet i informationssystem genom att logga följande säkerhetsrelaterade händelser:
    a. obehörig åtkomst eller försök till åtkomst i IT-miljöer och informationssystem.
    b. förändringar av konfigurationer och säkerhetsfunktioner som kräver privilegierade rättigheter.
    c. förändringar av behörigheter för användare och system.
    d. åtkomst till information som kräver utökat skydd.
2. Analysera säkerhetsloggar för att upptäcka och hantera incidenter och avvikelser.
    a. säkerhetsloggarna ska:
    b. möjliggöra utredning av intrång, tekniska fel och säkerhetsbrister.
    c. vara utformade så att de kan jämföras mellan olika loggar.
    d. vara tillgängliga för analys under fastställd bevarandetid.
3. Dokumentera
    a. Hur säkerhetsloggarna ska användas.
    b. Var loggningsuppgifter hämtas ifrån.
    c. Var säkerhetsloggarna lagras.
    d. Hur loggarna skyddas.
    e. Hur länge loggarna ska bevaras.

Organisationen bör...

1. Säkerställa att säkerhetsloggar innehåller information om:
2. Vem eller vad som agerat.
3. Vad som har hänt.
4. Tidpunkten för händelsen.
5. Skapa jämförbarhet genom att använda organisationens tidstjänst för alla säkerhetsloggar.
6. Samla säkerhetsloggar i ett särskilt avsett informationssystem.

4.11 Övervakning

Syfte

För att upptäcka och hantera intrång och avvikelser som kan påverka säkerheten, behöver organisationen övervaka säkerhetsrelaterade händelser i sina informationssystem.

Krav

Organisationen ska identifiera och hantera behovet av...

1. Intrångsdetektering.
2. Intrångsskydd.
3. Realtidsövervakning av informationssystem.

Organisationen bör bedöma behovet av intrångsdetektering och intrångsskydd för...

1. Enskilda informationssystem.
2. Den övergripande produktionsmiljön.
3. Utvecklings-, test- och utbildningsmiljöer.

Övervakning är särskilt viktig i informationssystem med koppling till externa nätverk, exempelvis e-post, webbsidor, webbtjänster och DNS-servrar. **Det är därför lämpligt att övervaka:**

- Nätverkstrafik
- Säkerhetsfunktioner
- Konfigurationer
- informationssystem som behandlar
- information i behov av utökat skydd
- informationssystem som av andra skäl
- bedöms ha behov av övervakning.

4.12 Skydd mot skadlig kod

Syfte

För att förhindra installation, spridning och exekvering av skadlig kod såsom virus, maskar, trojaner, spionprogram och utpressningsprogram, behöver organisationen skydda sin IT-miljö mot skadlig kod.

Krav

Organisationen ska använda mjukvara som ger skydd mot skadlig kod. För informationssystem där sådan mjukvara inte finns tillgänglig ska andra åtgärder vidtas.

Antivirus mot skadlig kod

Skadlig kod sprids ofta genom att användare luras att klicka på länkar eller öppna e-postbilagor med makron. Organisationen kan också få in skadlig kod via informationsdelning med andra. Spridningssätt, konsekvenser och vilka system som är mest utsatta förändras ständigt. Därför är det viktigt att omvärldsbevaka utvecklingen av skadlig kod och hålla koll på vilka system den angriper.

Det finns två olika sätt att skydda sig mot skadlig kod med hjälp av mjukvara (antivirus-program) - svartlistning och vitlistning.

Svartlistning är en vanlig funktion i antivirusprogram, men för att vara effektiv måste leverantören snabbt tillhandahålla uppdateringar när ny skadlig kod upptäcks. Före uppdateringen är organisationen oskyddad mot den nya koden. Skyddet förbättras genom vitlistning, men det kräver ett strukturerat arbetssätt för att tillåta nödvändig mjukvara samtidigt som skadlig kod blockeras. För att minimera påverkan på användarna är det bra att använda vitlistningens inlärningsläge under en övergångsperiod.

4.13 Skydd av utrustning

Syfte

För att förhindra skador på och obehörig åtkomst till it-utrustning, behöver organisationen säkerställa ett tillräckligt fysiskt skydd.

Krav

Organisationen ska skydda den utrustning som informationssystem består av mot skador och obehörig åtkomst, genom att...

1. Placera servrar och nätverksutrustning på säkra platser.
2. Ge behörighet till IT-utrymmen endast till de som behöver det.
3. Övervaka och sätt upp larm i IT-utrymmen.
4. Registrera vem som går in i IT-utrymmen och spara informationen under viss tid.
5. Ha regler för hur mobil utrustning ska skyddas.

4.14 Redundans och återställning

Syfte

För att kunna fortsätta verksamheten vid incidenter och avvikelser utan större störningar behöver organisationen se till att det finns tillräcklig redundans (dvs. backup-lösningar och alternativa system) och förmåga att återställa informationssystem snabbt.

Krav

För att säkerställa tillgång till information och system vid incidenter, bör organisationen...

1. Ha regler för hur hela produktionsmiljön och enskilda informationssystem ska återställas.
2. Öva återställning av centrala informationssystem som är avgörande för verksamheten.
3. Placera centrala servrar och nätverksutrustning i olika IT-utrymmen för att skapa redundans.

Organisationen bör även ha regelbunden övning av återställning, baserat på behovet av tillgänglighet.

Vill ni ha rådgivning gällande NIS2?

Hör av er till oss på sales@gridheart.com