Säkerhetsföreskrifter

Gäller från 1.1.2018.

Cyber försäkring säkerhetsföreskrifter S711

290104s 01.18

1 Syfte

De här säkerhetsföreskrifterna är avsedda att fogas till försäkringsavtalet för att komplettera de egentliga försäkringsvillkoren. I anvisningarna ingår skyddstekniska bestämmelser och råd och då de följs kan de förhindra att skador uppstår och minska på skadebeloppen.

2 Förpliktelse

De här säkerhetsföreskrifterna utgör en del av försäkringsavtalet. Försäkringstagaren och den försäkrade ska iaktta de här säkerhetsföreskrifterna och dess bestämmelser. Om säkerhetsföreskrifterna inte iakttas, kan ersättningen nedsättas eller helt avslås enligt lagen om försäkringsavtal.

Försäkringstagaren är skyldig att se till att de personer som arbetar på företaget känner till innehållet i den här anvisningen.

De här anvisningarna i anslutning till cybersäkerhet är avsedda främst för små och medelstora organisationer, som inte nödvändigtvis har möjligheter att anställa egen eller utomstående cybersäkerhetspersonal, som granskar och förbättrar hanteringen av cyberrisker

3 Anvisningar för cybersäkerhet

3.1 Utveckling och upprätthållande av informationssäkerhetspolicy

Organisationen ska fastställa och dokumentera informationssäkerhetspolicyn eller komplettera sin existerande informationssäkerhetspolicy så att den omfattar åtminstone följande områden:

Klassificering av data och datasystem

Hur uppgifter klassificeras, hurdan informationssäkerhet som ska iakttas vid behandling av uppgifter på olika nivåer, med hurdana datasystem ska uppgifter behandlas.

Roller och ansvar i anslutning till informationssäkerhet

I informationssäkerhetspolicyn ska tydligt fastställas roller och ansvar i anslutning till informationssäkerhet: vem svarar för informationssäkerheten, vem fungerar som informationssäkerhetsansvarig, vem har behörighet att behandla information på olika plan, vem svarar för informationssäkerheten i system och datalager och vem administrerar behörigheten att behandla.

Behandling och tryggande av personuppgifter

Om en organisation samlar person- eller kunduppgifter, ska man i informationssäkerhetspolicyn fastställa handlingsmodeller, med vilka personuppgifter behandlas i enlighet med personregisterlagen och EU:s dataskyddsförordning.

Anvisningar för användning av sociala medier och datanät

I informationssäkerhetspolicyn finns anvisningar och begränsningar för personalen om användning av sociala medier och datanät.

Underhåll och uppdatering

I informationssäkerhetspolicyn ska fastställas hur den upprätthålls och uppdateras samt den instans som godkänner ändringar. I den ska också fastställas, hur policyn effektivt ges samtliga anställda i organisationen och övriga relevanta intressentgrupper för kännedom.

I informationssäkerhetspolicyn eller informationssäkerhetsanvisningarna kan också behandlas mer detaljerat de ärenden som nämns nedan i punkterna 3.2–3.11.

3.2 Informationssäkerhet och integritetsskydd

Organisationen ska gällande data och informationssäkerhet reda ut åtminstone följande:

- Hurdan data organisationen använder och förvarar i sin verksamhet. Finns det t.ex. kunddata, kontouppgifter, uppgifter om finansiella transaktioner, kontaktinformation, uppgifter i anslutning till köpbeteende, bankförbindelseuppgifter, kortbetalningsuppgifter, löneuppgifter, skatteuppgifter, personuppgifter, hälsouppgifter, patientuppgifter, affärshemligheter o.dyl. konfidentiell information om kunder, anställda eller andra intressentgrupper.
- Hur behandlas denna information och hur är den skyddad.
- Vem har tillgång till uppgifterna och under vilka förutsättningar. Vem har behov av tillgång till konfidentiella uppgifter för att sköta sitt arbete och vem behöver inte tillgång till konfidentiella uppgifter. Hurdana användar- och åtkomstbehörigheter har olika parter.
- Vilka datasystem eller uppgifter är kritiska för kontinuiteten i affärsrörelsen.

Utifrån det ovan nämnda ska uppgifterna klassificeras enligt sin konfidentialitet exempelvis i följande klasser, som baserar sig på instruktionen i vm.fi/sv/vahti-verksamheten:

- Ytterst hemlig
- Hemlig
- Konfidentiell
- Begränsad tillgång
- Offentlig

Då uppgifterna är klassificerade, ska för varje klass fastställas åtkomsträttigheter och principerna för informationssäkerheten i regel så, att ju mer hemlig och kritisk information det är fråga om, desto färre ska ha åtkomstbehörighet till den och desto bättre ska informationen vara skyddad (t.ex. med lösenord, kryptering och vid behov med identifieringsverktyg eller biometriska identifikatorer).

Försäkringstagaren ska dagligen se till att det finns uppdaterade säkerhetskopior av filerna. Säkerhetskopiorna ska förvaras i andra lokaliteter än ursprungliga data och säkerhetskopiorna ska vid behov också krypteras.

Säkerhetskopieringen av data ska också ordnas så att alla data som är viktiga för verksamheten ska vid behov kunna återskapas från säkerhetskopior. Man ska regelbundet testa att data kan återskapas från

säkerhetskopior, för att säkerställa att säkerhetskopiorna fungerar och att processen med återskapandet fungerar. Man ska fastställa vem som ansvarar för säkerhetskopieringen, vilka data ska säkerhetskopieras, med vilka verktyg, hur ofta, hur säkerhetskopiorna förvaras och vem som har tillgång till säkerhetskopiorna.

Instruktioner ska upprättas i händelse av dataintrång eller om data förstörs och instruktionerna ska ges alla för kännedom som arbetar med data.

3.3 Informationssäkerhetspraxis för anställda

För de anställda ska fastställas deras behörighet i anslutning till deras arbetsroller att få tillgång till data och datasystem. Om personen inte har behov av att behandla konfidentiell information i sina arbetsuppgifter, ska personens tillgång till sådan information förhindras. Om arbetsuppgiften förutsätter behandling av konfidentiell information, ska från fall till fall fastställas varje persons åtkomsträttigheter och begränsa dem till sådana uppgifter och system som skötseln av arbetsuppgiften kräver.

Kunddata eller andra konfidentiella uppgifter får inte granskas, om det inte finns ett arbetsrelaterat behov att granska dem. Uppgifter kan inte överlåtas till tredje part, om man inte är helt säker på personens identitet och behörigheter att granska ifrågavarande uppgifter.

Informationssäkra dataöverföringsmetoder ska alltid användas och vid behov ska information krypteras, om den sänds till allmän e-post.

Konfidentiell information (i elektronisk form eller som papperskopior) ska förvaras endast så länge som det behövs eller den enligt bestämmelserna ska förvaras. Man ska se till att informationsmaterial som är föråldrat eller som annars ska förstöras förstörs på ett informationssäkert sätt.

Alla anställda ska iaktta rena bordets politik, så att dokument som innehåller konfidentiell information inte är tillgängliga för utomstående som eventuellt kommer in i lokaliteterna.

Alla anställda ska genomgå utbildning inom informationssäkerhet, där man går igenom organisationens informationssäkerhetspolicy, säker användning av datateknik och de centrala informationssäkerhetsriskerna och verktyg för hantering av dem. Repetitionsutbildning ska ordnas regelbundet eller alltid då det finns behov av att informera om nya hot eller metoder i anslutning till informationssäkerhet.

Sådana rutiner ska införas, att om en person slutar arbeta i organisationen ska personens åtkomsträttigheter till system och data genast fråntas då anställningen upphör.

3.4 Bedrägerier och svindleri

Elektronisk informationsförmedling och internet ger brottslingar många nya möjligheter att göra bedrägerier eller att lura antingen organisationen eller dess kunder. En del av den här typen av brott omfattas inte i försäkringstekniskt avseende av cyberförsäkringen utan de ersätts ur traditionella brottsförsäkringar. Centrala skyddande åtgärder är bl.a.:

- öppna inte suspekta e-postbilagor eller länkar
- i datorer får inte installeras programvara, vilkas funktion och syfte eller ursprung det inte finns mer detaljerad information om. Endast huvudanvändarna borde ha behörighet att installera program i datorer.
- operativsystemet, antivirusprogram, brandmurar och andra program ska alltid vara uppdaterade med de senaste säkerhetsuppdateringarna. Automatiska uppdateringar ska användas i alla program, där det är möjligt.
- de anställda ska vara utbildade i att identifiera bedrägeriförsök och nätfiske (phishing, social engineering)
- identiteten på personer som per telefon ber om personlig information ska alltid kontrolleras genom att man ringer tillbaka till det kända, riktiga telefonnumret
- kunderna har underrättats om att de aldrig blir tillfrågade om sekretessbelagd, personlig information (lösenord, bankförbindelseuppgifter, betalkortsuppgifter m.m.), per telefon eller e-post
- man ska undvika att använda minnespinnar och andra mobila lagringsmedier och de ska alltid kontrolleras med ett antivirusprogram i händelse av skadliga program
- För att undvika spionprogram ska länkar till pop up-fönster på webbplatser inte öppnas

3.5 Datanätets säkerhet

Organisationens nät ska avskiljas från det allmänna nätet med brandmurar och proxyservrar i alla kontaktytor mot det allmänna nätet. Antivirusprogram och program som observerar försök till intrång ska användas vid behov vid varje kontaktyta, så att en tillräcklig säkerhetskontroll uppnås.

Om molntjänster används, ska man säkerställa att tjänsteleverantören ger åtminstone ett lika gott skydd för den information som finns i tjänsten som det egna nätet ger. Det ska säkerställas att i tjänsteavtalet har fastställts tjänsteleverantörens ansvar, kvaliteten på den tjänst som ges, tid för att återskapa data och eventuella säkerhetskopieringstjänster samt möjlighet att auditera tjänsten.

Det ska skapas rutiner för lösenord, som förutsätter att de anställda använder tillräckligt starka (vid behov finns anvisningar exempelvis på Kommunikationsverkets webbplats) lösenord, som byts regelbundet och som endast användarna själva känner till.

Tillgång till trådlösa nät (WLAN) ska vara begränsat endast för apparater och användare som organisationen fastställt. Det trådlösa nätet ska ha en kryptering av minst nivån WPA2.

Om ett trådlöst nät är tillgängligt för besökare, ska den vara avskild från organisationens eget nät, så att man inte genom gästnätet får tillträde till uppgifter och applikationer i organisationens nät.

Allt som har klassificerats som hemligt eller konfidentiellt ska i mån av möjlighet hållas hemligt. Om företaget har nätsidor, ska skyddet av dem säkerställas.

Alla system och program på nätet ska uppdateras alltid med de nyaste programversionerna och -uppdateringarna, då de är tillgängliga. Det lönar sig att använda automatiska uppdateringar särskilt för virusbekämpning, för bekämpning av skadliga program och i program i anslutning till brandmurar.

Tillträde till sådana webbplatser som de anställda inte har något behov av i sitt arbete, är det skäl att begränsa. Inställningarna i webbläsarna ska vara sådana att man inte via det interna nätet kommer in på förbjudna webbplatser.

Om distansförbindelser används, ska man se till att de är informationssäkra. Vid distansanvändning ska användas säkra förbindelser och stark identifiering, där som tilläggsverifiering används separata varierande lösenord eller fasta identifieringsverktyg.

I informationssäkerhetspolicyn ska alla informeras om att okända minnespinnar eller andra mobila lagringsmedier inte får anslutas till datorer eller mobilapparater som är kopplade till nätet innan de granskats i händelse av skadliga program.

3.6 Säkerheten hos hemsidor och webbservrar

Webbservrar genom vilka kunderna ges information och tjänster, hör till de vanligaste objekten för cyberattacker. Webbservrar, deras programplattformar och därtill hörande nätinfrastruktur ska skyddas omsorgsfullt mot dataintrång, blockeringsattacker och obehörig användning.

Vid planering av en webbtjänst som är öppen för kunderna ska man ta hänsyn till de säkerhetsresurser som krävs. Man ska se till att utrustnings- och programlösningarna möjliggör en tillräcklig säkerhetsnivå och att det finns tillgång till tillräcklig kompetens för att upprätthålla och uppdatera säkerhetsnivån.

Då en webbtjänst genomförs ska man beakta att fabriksinställningarna av säkerhetsnivån hos utrustning och program ofta har ställts in för att stöda enkel och snabb användning och inte nödvändigtvis med tanke på en tillräcklig säkerhetsnivå. Det är skäl att noggrant gå igenom säkerhetsinställningarna i systemet och ändra på dem så att

de motsvarar organisationens behov. Särskilt viktigt är det att byta ut alla förhandsinställda lösenord till starka lösenord som motsvarar organisationens informationssäkerhetspolicy och se till att de nyaste informationssäkerhetsuppdateringarna är i användning. Det är skäl att ur nättjänsten avlägsna onödiga tjänster och applikationer samt onödigt innehåll. Det är också skäl att med tester säkerställa informationssäkerheten i nättjänsterna och -innehållet.

Det är också skäl att försäkra sig om att i nättjänsten endast publiceras behörig, nödvändig och saklig information. Om det i tjänsten måste publiceras sekretessbelagd information eller personuppgifter, ska vid publiceringen av dem tillämpas en särskild hög säkerhetsnivå. Vid behov ska känslig information hemlighållas och identifieringen av användarna ska vara tillräckligt verifierad.

Det ska säkerställas att information som publiceras på webbtjänsten är oförvanskad. Man ska se till att olovligt brukande eller ändring av uppgifter har förhindrats tillräckligt effektivt.

Upprätthållandet av säkerheten i webbservern kräver regelbundna åtgärder, för vilkas vidtagande ska beredas tillräckliga resurser, såsom:

- upprätthållande och analys av logguppgifter
- installation och testning av de senaste uppdateringarna och korrigeringarna
- regelbunden säkerhetskopiering av kritiska data
- skapande av återställningsrutiner i händelse av störningar
- regelbunden testning av säkerheten i nättjänsten.

3.7 Säkerheten i e-post

E-post är för många organisationer mycket viktig för att den dagliga verksamheten ska fungera. För säkerheten i e-post ska bl.a. följande aspekter beaktas:

För kontroll av all e-post ska användas skräppostfilter och antivirusskydd. Dessutom ska man ombesörja att filtren och antivirusskyddet automatiskt uppdateras till de nyaste versionerna. Inställningarna i skräppostfiltren ska kontrolleras regelbundet, så att de inte i misstag hindrar att nödvändiga e-postmeddelanden kommer fram.

Alla anställda som använder e-post ska utbildas i hur man använder e-post säkert. Personalen måste kunna identifiera risker i anslutning till användningen av e-post och förstå när och hur e-post kan användas i arbetsuppgifter och när det är skäl att be om hjälp av en expert.

Konfidentiell information sänds per e-post endast till de instanser som har rätt att använda informationen. Det ska fastställas hurdan information som inte får sändas med e-post och hurdan information som med e-post ska sändas i krypterad form.

3.8 Mobilapparater

I fråga om informationssäkerheten i mobilapparater är det viktigt att se till bl.a. följande:

Användning av informationssäkerhetsapplikationer i samtligamobilapparater

Det vore bra om man i samtliga telefoner och surfplattor skulle använda informationssäkerhetsprogram som är utvecklade för dem, om sådana är tillgängliga.

Uppdatering av programvara

Precis som i fasta apparater, ska man för mobilapparaters del se till att programvara och informationssäkerhetsapplikationer har de senaste uppdateringarna.

Användning av lösenord i telefoner och andra mobilapparater

I mobilapparater ska i mån av möjlighet användas starka lösenord på samma sätt som i fasta terminaler. Mobilapparater ska inställas så att de låser sig automatiskt, om de inte används.

Hemlighållande av information som finns i mobilapparat

Den information som finns i mobilapparater ska hemlighållas, så att om apparaten förkommer eller hamnar i fel händer kommer man inte åt informationen.

Beaktandet av miljön

Användare av mobilapparater ska förhindra att konfidentiell information eller lösenord syns till utomstående då apparaten används.

Användning av e-post och sociala medier i mobilapparater

Vid användning av e-post och sociala medier ska iakttas motsvarande säkerhetsbestämmelser som med fasta apparater.

Handlingsmodell om mobilapparat blir stulen eller förkommer

En handlingsmodell ska utarbetas i händelse av att en mobilapparat blir stulen eller förkommer. Användarna ska känna till hur de ska ta apparaten ur bruk och skydda uppgifterna i den.

Tömning av mobilapparater som tagits ur bruk

Om apparater tas ur bruk, ska man försäkra sig om att uppgifterna i dem avlägsnas oåterkalleligt. Också SIM-kort som tagits ur bruk ska förstöras på ett informationssäkert sätt.

3.9 Lokalitetssäkerhet och operativ säkerhet

Inom lokalitetssäkerhet och operativ säkerhet ska beaktas bl.a. följande aspekter i anslutning till informationssäkerhet:

Den fysiska säkerheten i lokaliteterna ska ordnas så att riskerna för apparatstölder och informationsläckage minimeras.

Datahanteringsutrustning som lätt kan tas med (bärbara datorer, surfplattor, smarttelefoner) får inte förvaras på platser, som kan nås från allmänna rum. Vid behov kan användas exempelvis kabellås, om apparaterna måste förvaras i rum, som lätt kan nås. I apparaterna kan också installeras spårningsprogram.

Det ska vara förbjudet att förvara användarkoder och lösenord i närheten av apparaten.

Skärmar till system som behandlar konfidentiell information ska placeras så att de inte syns till rum där utomstående har tillträde.

Skydd av konfidentiellt material som skrivs ut

I mån av möjlighet ska man undvika att skriva ut konfidentiellt material. Pappersutskrifter ska förvaras i låsbara arkivskåp eller kassaskåp. Skrivare, med vilka konfidentiellt material utskrivs borde förses med ett program som tillåter utskrivning endast för en användare som identifierar sig då användaren hämtar utskrifterna, så att inga utskrifter blir liggande i skrivaren eller i dess närhet.

Säkerheten hos brevpost

Också i fråga om brevpost ska informationssäkra rutiner för sändning och mottagning utarbetas. Konfidentiell brevpost får inte hamna i omständigheter, där dess informationssäkerhet kan äventyras.

Informationssäker förstöring av sopor

Man ska se till att sopor förstörs på ett informationssäkert sätt. Rutiner ska utarbetas så att material som innehåller konfidentiell information förstörs på ett informationssäkert sätt med dokumentförstörare eller samlas in i låsbara behållare för destruktion.

Datorer, surfplattor, smarttelefoner eller datalagringsutrustning som ska förstöras eller återvinnas ska på ett informationssäkert sätt tömmas på konfidentiell information, det räcker inte med att enbart förstöra filerna.

3.10 Säkerheten med betalningsuppgifter

Om en organisation erbjuder kunderna möjlighet till kortbetalningar eller nätbetalningar, ska organisationen ombesörja säkerheten hos de uppgifter som sparas i detta sammanhang. Vanligtvis är det en utomstående producent av betaltjänster som producerar tjänsten och som också behandlar kort- och betalningsuppgifterna samt ombesörjer deras informationssäkerhet. Om organisationen i samband med betalningar för egna syften sparar information om kunder, kort eller konton exempelvis i anslutning till ett kundregister, ska man särskilt noggrant i alla skeden av processen se till att dessa uppgifter behandlas på ett informationssäkert sätt. Om det är möjligt att ersätta kortnummer och personlig information om kunden som samlas för

annat än betalningssyften med andra koder, så lönar det sig absolut att göra detta.

Endast utrustning och program som är godkända för användning i betalningssystem ska användas. Man ska förhindra att utomstående kan göra ingrepp på betalterminaler, så att de inte kan montera skimningsutrustning med vilka kortuppgifter kan kopieras.

Inom organisationens egen betalningsrörelse ska endast användas godkända program eller applikationer för betalningsförmedling. Tillträde till betalapplikationer ska begränsas till endast de personer som i sitt arbete har behov av att göra betalningar. Om det är nödvändigt att använda betalningssystem på distans ska förbindelserna vara krypterade.

Leverantören av betalningssystemet kan i informationssäkerhetsfrågor som gäller betalningssystem och -program i de flesta fall ge mer detaljerade råd och handledning i hur de används på ett informationssäkert sätt.

3.11 Förberedelser mot dataskyddskränkningar eller cyberattacker

I händelse av dataskyddskränkningar eller cyberattacker ska det finnas fastställda och dokumenterade handlingsmodeller och -anvisningar, så att man utan dröjsmål ska kunna reagera på rätt sätt om det sker en dataskyddskränkning.

Handlingsmodellen ska omfatta olika typer av cyberhot, exempelvis: stöld av utrustning, utrustning som går sönder eller förkommer, systemintrång, skadliga program, virusprogram, blockeringsattacker, datastölder eller dataläckage samt cyberutpressning.

Information om krav på förberedelser vid informationssäkerhetskränkningar och avvikelser finns på anvisningssajten för ledningsgruppen för datasäkerheten inom statsförvaltningen (VAHTI) bl.a. i dokumentet 8/2017 Tietoturvapoikkeamatilanteiden hallinta eller i nyare versioner.