SSF Cybersäkerhet Bas

Sammanfattning och definitioner

Stöldskyddsföreningen

Sammanfattning och definitioner

Datorer och mobila enheter

Allmänt

- standardlösenord för alla användarkonton till datorer och mobila enheter ska ändras till starka lösenord som inte återanvänds

  Anm. Inga lösenord ska återanvändas (gäller såväl tidigare använda lösenord som användande av samma lösenord på olika enheter) av varken medarbetare eller grupper av medarbetare.

- Lösenord som använts inom organisationen ska inte användas privat, eller vice versa.
- starka lösenord ska vara definierade i ett beslut av organisationen. Lösenord ska minst uppfylla säkerhetsnivån enligt denna norm
- kryptering av lagringsutrymme på datorer och mobila enheter ska vara aktiverad där så är möjligt.

Säkerhetskopiering

- information ska säkerhetskopieras i den omfattning verksamheten beslutat
- minst en säkerhetskopia ska vara tillgänglig endast för personer med administrativ systembehörighet.

  Anm. Kontroll av säkerhetskopierad information kan ske genom regelbundna stickprovskontroller.

Skydd mot skadlig kod

Programvara för skydd mot skadlig kod:

- ska vara installerad på alla datorer och mobila enheter som är anslutna till eller kan ansluta till externa nätverk, t.ex. Internet.
- ska uppdateras automatiskt eller genom särskild rutin
- ska vara konfigurerad för att automatiskt genomsöka filer vid åtkomst (inklusive vid hämtning och öppning av filer på nätverksenheter och flyttbara lagringsmedia)
- ska på datorer skanna och varna om webbplatsen innehåller skadlig kod

  Anm. Programvaran ska genom varning eller blockering säkerställa att användaren uppmärksammas på webbsidor som innehåller skadlig kod, och förhindra att koden exekveras i ett initialt skede.

- ska vara konfigurerad för att genomföra regelbundna skanningar efter skadlig kod.

Användning av organisationens resurser för privat bruk

- det ska vara beslutat om och i vilken omfattning organisationens resurser får användas för privat bruk.

Användning av privat utrustning

- det ska vara beslutat om och i vilken omfattning privat utrustning får användas i organisationens verksamhet
- privat utrustning som används i organisationen ska omfattas av samma säkerhetskrav som organisationens utrustning i övrigt.

Mjukvaror och applikationer

Allmänt

- all mjukvara som omfattas av upphovsrätt ska vara licensierad för användning i organisationens verksamhet
- mjukvara ska om möjligt alltid laddas ned från den officiella distributörens hemsida eller liknande verifierbara källor
- applikationer till mobila enheter får endast laddas ned från betrodda källor
- endast mjukvaror och applikationer som är nödvändig för verksamheten ska installeras
- mjukvaror och applikationer som inte används ska avinstalleras så snart som möjligt.

  Anm. Att ladda ner applikationer till mobiltelefoner och surfplattor från betrodda källor innebär exempelvis AppStore, Google Play Store eller organisationens egen interna plats för godkända program och applikationer.

Säkerhetsuppdateringar

- säkerhetsuppdateringar ska installeras automatiskt för operativsystem, programvaror och applikationer som körs på datorer, nätverksenheter och mobila enheter, där det är tekniskt möjligt
- operativsystem, programvaror, applikationer och nätverksenheter som inte längre säkerhetsuppdateras ska tas bort eller flyttas till logiskt eller fysiskt separerade segment där de kan hanteras utifrån särskilda regler.

  Anm. Om kravet inte uppfylls ska organisationen motivera varför man accepterar risken med att frångå ovanstående krav.

Automatisk programstart och automatisk uppspelning

- automatisk programstart ska vara begränsat till applikationer som är identifierade av organisationen som nödvändiga att starta automatiskt

  Anm. De identifierade applikationerna ska vara beslutade av organisationen.

- automatisk uppspelning ska vara avstängt för alla filer från portabla lagringsmedier.

Nätverk

Allmänt

- en eller flera nätverksenheter med brandväggsfunktionalitet ska vara installerade mellan företagets interna nätverk och externa nätverk t.ex. internet

  Anm. I de fall det inte finns ett internt nätverk ska datorer vara försedda med brandväggsfunktionalitet mellan dator och externa nätverk, t.ex. Internet.

- innan en nätverksenhet installeras ska standardlösenordet ändras till ett starkt lösenord som inte återanvänds, där så är tekniskt möjligt

Anm. Inga lösenord ska återanvändas (gäller såväl tidigare använda lösenord som användande av samma lösenord på olika enheter) av varken medarbetare eller grupper av medarbetare.

- Lösenord som använts inom organisationen ska inte användas privat, eller vice versa.
- lösenordsändringar för administrativa konton (inklusive servicekonton) i nätverksenheter ska ske enligt intervall beslutade av organisationen
- alla öppna anslutningar (dvs. tillåtna portar och tjänster) på brandväggen ska vara beslutade av organisationen

  Anm. Beslutet bör dokumenteras (inklusive en förklaring av verksamhetsbehov)
- brandväggsregler som inte längre behövs ska tas bort eller inaktiveras
- datorer som inte behöver ansluta till Internet ska förhindras från att initiera anslutningar till Internet
- det administrativa gränssnittet som används för att konfigurera organisationens brandvägg eller brandväggar ska inte vara åtkomligt från externa nätverk, t.ex. Internet
- samtliga trådlösa nätverk ska vara krypterade och skyddas av ett säkert protokoll och med ett starkt lösenord eller certifikat.

  Anm. Med säkert protokoll avses ett protokoll i linje med rådande god sed. För närvarande rekommenderas WPA2-PSK(AES) eller motsvarande.

Gästnätverk

- gästnätverk ska vara avskilt från organisationens interna nätverk.

  Anm 1. Lösenordet till gästnätverket delges enbart behöriga.

  Anm 2. Ordinarie arbete ska inte ske via gästnätverket.

Trafikskydd

- vid användande av allmänna nätverk (så som offentligt Wi-Fi och trådbundna allmänna nätverk) ska trafiken skyddas från obehörig insyn med hjälp av VPN eller motsvarande
- kommunikation mellan klient och servrar för e-post ska vara skyddad med kryptering

  Anm. Kryptering kan ske med hjälp av TLS (Transport Layer Security).
- organisationens domännamn för DNS ska skyddas med DNSSEC.

Externa it-tjänster inkl. molnlagring

Avtal

- vid nyttjande av externa it-tjänster och molntjänster ska det finnas ett juridiskt bindande avtal mellan organisationen och leverantören.

Avtalets omfattning

Avtalet ska normalt omfatta följande villkor:

- vem som äger informationen
- vem som har access till informationen
- var (geografiskt) informationen lagras
- vilken servicenivå (tillgänglighet, support, felavhjälpning etc.) organisationen kan förvänta sig av leverantören och avtalade leveranser (tillgänglighet på t.ex. internet)
- att leverantören, genom ackrediteringar, certifikat eller andra oberoende bevis, har en säkerhetsnivå vilken motsvarar eller överstiger kraven enligt denna norm
- hur säkerhetsincidenter hanteras av leverantören och rapporteras till beställaren
- att informationen säkerhetskopieras och hur återställning genomförs
- om och på vilket sätt informationen krypteras

GDPR

- i det fall tjänsten omfattar behandling eller lagring av personuppgifter ska leverantören intyga att denne uppfyller kraven enligt den europeiska dataskyddsförordningen (GDPR)
- ett personuppgiftsbiträdesavtal ska finnas mellan leverantören och organisationen om detta så krävs.

Behörigheter

Användarkonton

- skapande av användarkonton ska ske efter beslut av organisationen

  Anm. Beslutet bör vara dokumenterat.
- systemadministratörsbehörighet får endast tilldelas och användas av personer som utför systemadministrativa tjänster
- administrativa konton ska endast användas för att utföra tillåtna administrativa aktiviteter, t.ex. systemunderhåll
- användarkonton ska vara tilldelade enskilda medarbetare
- användarkonton ska tas bort eller inaktiveras när de inte längre behövs (t.ex. när en medarbetare ändrar roll eller lämnar organisationen).

Åtkomst

- enskilda medarbetare ska endast ha åtkomst till de system arbetsuppgifterna kräver
- delade lagringsytor ska vara konfigurerade så att enskilda medarbetare endast har åtkomst till den information arbetsuppgifterna kräver.

Lösenord

- användare ska, som minimum, autentiseras med starka lösenord som inte återanvänds, innan åtkomst beviljas till program och datorer
- lösenordsändringar för systemadministratörskonton och servicekonton ska ske enligt intervall beslutade av organisationen
- om det misstänks eller kan konstateras att lösenord har blivit känt för någon annan än användaren själv ska det omedelbart bytas ut
- lösenord ska bytas ut i den omfattning och med den regelbundenhet som verksamheten kräver

Utbildning i informationssäkerhet

- Samtliga medarbetare ska genomföra grundläggande utbildning i informations-säkerhet i form av DISA – Datorstödd informationssäkerhetsutbildning för användare (Myndigheten för Samhällsskydd och Beredskap, MSB) eller utbildning med motsvarande omfattning.

Definitioner

För tillämpning av detta dokument gäller de definitioner, termer och förkortningar som anges nedan.

Användarkonto (user)

Konto med minsta möjliga behörigheter, för att lösa sina arbetsuppgifter och som används för arbete i icke-systemadministrativa sysslor.

Applikation

Avser ett program som syftar till att utgöra länken mellan datorns operativsystem och användaren. Exempel på detta är Microsoft Excel, Google Chrome, Adobe Photoshop, Spotify och McAfee Antivirus.

Behörighet

Tilldelade rättigheter att använda en informationstillgång på ett specificerat sätt. Exempel på rättigheter som kan tilldelas är att läsa, skapa, ändra eller ta bort information.

Dator

Avser såväl bärbara datorer, stationära datorer som servrar eller motsvarande.

Mobila enheter

Avser såväl mobiltelefoner, surfplattor (tablets) som wearables (t.ex. smarta klockor) eller motsvarande.

Nätverksenhet

Avser routrar, brandväggar, managerbara switchar och motsvarande. Det avser också alla enheter, undantaget gästenheter i gästnätverket, som är anslutna till organisationens nätverk och som inte är specificerade under 3.3 dator eller 3.4 mobila enheter. Exempel på detta är nätverksanslutna övervakningskameror, skrivare, och smarta enheter.

Organisationens resurser

Avser resurser som ägs eller hanteras av organisationen i organisationens infrastruktur/miljö.

Operativsystem

Avser ett eller flera program som syftar till att utgöra länken mellan datorns hårdvara och användarens programvara. Exempel på detta är Windows 7/8/10, Linux och Mac OS X.

Portabla lagringsmedier

Avser USB-minnen, externa hårddiskar, CD- och DVD-skivor eller motsvarande.

Programvara

Avser mjukvara i betydelsen organiserad samling av data och maskininstruktioner vilka utför en uppgift på ett datorsystem. I detta inkluderas både operativsystem och applikationer, men även programmeringsverktyg och andra program som faller utanför definitionerna ovan.

Servicekonton

Servicekonton avser konton som varken används av administratörer eller användare, utan av tjänster som behöver ett konto för exempelvis tillgång. Exempel på detta är ett konto tillhörande en databastjänst som behöver skrivrättigheter på en server eller ett konto tillhörande ett antivirusprogram som behöver kunna läsa användares filer.

Starka lösenord

Ett starkt lösenord ska: inte förekomma i kända lösenordsdumpar/lösenordslistor, innehålla minst 10 tecken. Lösenordet ska bestå av gemener, versaler och specialtecken, och inte innehålla ett ord förekommande i en ordbok eller motsvarande där substitution har förekommit (t.ex. utbyte av en bokstav i ett ord till en siffra).