Algemene regels

Incident en Datalekken

Incidenten en datalekken dienen z.s.m. gemeld te worden bij de Security Officer.

Verantwoordelijkheden gebruikersaccount

De gebruiker dient een andere persoon niet toe te staan, direct of indirect, gebruik te laten maken van zijn/haar toegangsrechten, d.w.z. gebruikersnaam, of te verlenen en mag de gebruikersnaam en/of wachtwoord niet van een ander gebruiken. Het gebruik van een groep van gebruikersnamen is verboden.
De eigenaar van het gebruikersaccount is de gebruiker ervan, die verantwoordelijk is voor het gebruik ervan en alle transacties uitgevoerd door dit gebruikersaccount.

Sessie

Inactieve gebruikerssessies moeten automatisch worden gesloten na 24 uren van inactiviteit.

Registratie en uitschrijving van gebruikers

Voor de inrichting hiervan gelden de volgende regels:

a. Gebruikers worden vooraf geïdentificeerd en geautoriseerd. Van de registratie wordt een administratie bijgehouden.
b. Op basis van een risicoafweging wordt bepaald waar en op welke wijze functiescheiding wordt toegepast en welke toegangsrechten worden gegeven.

De procedure voor registratie en afmelden van gebruikers moet omvatten:

a. Gebruik van unieke gebruikersidentificaties (ID) zodat gebruikers kunnen worden gekoppeld aan en verantwoordelijk kunnen worden gesteld voor hun handelingen;
b. Waarborgen dat overtollige gebruikers-ID's niet aan andere gebruikers worden uitgegeven.

Gebruikers toegang verlenen

De procedure voor het verlenen van toegang moet omvatten:

a. Controleren dat het toegewezen toegangsniveau geschikt is;
b. Gebruikers een bevestiging van hun toegangsrechten geven;
c. Waarborgen dat er geen toegang verleend wordt totdat de autorisatieprocedures zijn voltooid;
d. Een formele registratie bijhouden van alle personen die zijn geregistreerd als gebruikers van de dienst;
e. Zo snel mogelijk intrekken of blokkeren van toegangsrechten van gebruikers die van functie of rol zijn veranderd, de organisatie hebben verlaten of hebben opgezegd.

Wachtwoorden

Ten aanzien van de kwaliteit van (tijdelijke) wachtwoorden dient het systeem af te dwingen dat gebruikers wachtwoorden kiezen die:

- tenminste tien tekens gebruiken
- tenminste één numeriek teken gebruiken
- tenminste één hoofdletter en tenminste een kleine letter gebruiken

- geen woord uit het woordenboek zijn , geen dialect of jargon woord van elke taal, evenmin een of meer van deze woorden achterstevoren geschreven
- niet zijn gebaseerd op privégegevens (bijv. geboortedatum, adres, naam familielid, enz.)
- de laatste drie keren niet zijn gebruikt

Capaciteitsbeheer

In het kader van het realiseren van de beveiligingseis omtrent beschikbaarheid is het raadzaam de noodzakelijke capaciteit (nu en in de toekomst) van diverse zaken in het oog te houden, opdat tijdig corrigerende maatregelen kunnen worden genomen. Gedacht kan worden aan: netwerk, bandbreedte, systeemgeheugen, en schijfgeheugen
Capaciteitseisen moeten vastgesteld worden voor elke nieuwe en bestaande activiteit.

a. Zorg voor afstemming daarop en controle van het systeem om de beschikbaarheid en doelmatigheid van de systemen te waarborgen en waar nodig te verbeteren.
b. Zorg voor detectiemaatregelen om problemen op tijd vast te stellen.
c. Betrek prognoses van toekomstige capaciteitsbehoeften bij nieuwe bedrijfs- en systeemeisen en huidige en geraamde trends in de informatieverwerkingscapaciteit van de organisatie.
d. Besteed bijzondere aandacht aan onderdelen met lange levertijden of hoge kosten.
e. Beheerders moeten het gebruik van de belangrijkste systeemonderdelen controleren en trends in het gebruik signaleren.

Beheersmaatregelen tegen malware

Baseer de bescherming tegen kwaadaardige programmatuur op het ontdekken en op herstelprogrammatuur, op een goed beveiligingsbewustzijn, toegangsbeveiliging van systemen en controle van wijzigingsbeheer.
Bescherming moet verkregen worden door:

a. Leveranciers van systeem- en applicatieprogrammatuur brengen geregeld ‘patches’ uit om fouten aan hun producten te verbeteren. Het is van belang alert te blijven op nieuwe ‘patches’.
b. Definiëren van beheerprocedures en verantwoordelijkheden voor de bescherming tegen kwaadaardige programmatuur op systemen, training in het gebruik ervan, rapportage en herstel van aanvallen met kwaadaardige programmatuur;
c. Opstellen van geschikte continuïteitsplannen voor herstel na aanvallen met kwaadaardige programmatuur, waaronder alle nodige voorzieningen voor back-ups van gegevens en programmatuur, evenals herstelmaatregelen.

Back-up

Houd geschikte back-upvoorzieningen beschikbaar, zodat alle essentiële gegevens en programmatuur kunnen worden hersteld na een computercalamiteit of een defect medium.

a. Definieer de eisen die aan back-up en herstel worden gesteld;
b. Houd nauwkeurige en volledige registers van back-ups bij en gedocumenteerde herstelprocedures;
c. Zorg dat de omvang (bijvoorbeeld volledige back-up of alleen van de wijzigingen) en frequentie van back-ups in overeenstemming zijn met de eisen en het kritieke karakter van de informatie;
d. Sla de back-ups op op een locatie die zich op zodanige afstand bevindt dat schade aan de back-up ten gevolge van een calamiteit op de hoofdlocatie onwaarschijnlijk is;

e. Zorg voor fysieke bescherming van de back-ups en de ruimte waarin deze zijn opgeslagen volgens dezelfde normen die gelden voor de hoofdlocatie; de beveiligingseisen voor media op de hoofdlocatie gelden ook voor de back-uplocatie;
f. Controleer en test herstelprocedures om te waarborgen dat ze doeltreffend zijn en dat ze kunnen worden uitgevoerd binnen de daarvoor volgens operationele herstelprocedures gestelde tijd;
g. Bescherm back-ups door middel van encryptie. Let er hierbij op, dat de back-up in geval van een calamiteit teruggeplaatst moet kunnen worden op een ander systeem.
h. Zorg ervoor dat altijd tenminste twee back-ups beschikbaar zijn.

Back-upprocedures kunnen worden geautomatiseerd om het back-up- en herstelproces te vereenvoudigen. Dergelijke geautomatiseerde oplossingen behoren voldoende te worden getest, voor implementatie en met regelmatige tussenpozen.

Beschermen van log- en auditbestanden

Logfaciliteiten en informatie in logbestanden moeten worden beschermd tegen vervalsing en onbevoegde toegang.

Kloksynchronisatie

De klokken van alle relevante informatie verwerkende systemen binnen een organisatie of beveiligingsdomein moeten worden gesynchroniseerd met één referentietijdbron. Gezondheidsinformatiesystemen die tijd kritische activiteiten voor gedeelde zorg ondersteunen, moeten in tijdssynchronisatiediensten voorzien om het traceren en reconstrueren van de tijdlijnen voor activiteiten waar vereist te ondersteunen.

Beheer technische kwetsbaarheden

a. Van softwarematige voorzieningen van de technische infrastructuur kan (bij voorkeur geautomatiseerd) gecontroleerd worden of de laatste updates (patches) in zijn doorgevoerd. Het doorvoeren van een update vindt niet geautomatiseerd plaats, tenzij hier speciale afspraken over zijn met de leverancier.
b. Indien een patch beschikbaar is, dienen de risico's verbonden met de installatie van de patch te worden geëvalueerd (de risico's verbonden met de kwetsbaarheid dienen vergeleken te worden met de risico's van het installeren van de patch).
c. Updates/patches voor kwetsbaarheden waarvan de kans op misbruik hoog is en waarvan de schade hoog is worden zo spoedig mogelijk doorgevoerd, echter minimaal binnen één week. Minder kritische beveiligings-updates/patches moeten worden ingepland bij de eerst volgende onderhoudsronde.

Beveiliging van netwerkdiensten

Tot de netwerkdiensten worden gerekend het leveren van aansluitingen, private netwerkdiensten, netwerken met toegevoegde waarde en beheerde beveiligingsoplossingen zoals firewalls en 'intrusion detection'. Deze diensten kunnen uiteenlopen van eenvoudige onbeheerde bandbreedte tot en met complexe aanbiedingen met toegevoegde waarde.
Beveiligingskenmerken van netwerkdiensten zijn:

a. Technologie toegepast voor de beveiliging van netwerkdiensten, zoals authenticatie, encryptie en netwerkverbindingscontroles;

b. Technische parameters vereist voor beveiligde verbinding met de netwerkdiensten in overeenstemming met de beveiligings- en netwerkaansluitingsregels;
c. Procedures voor het gebruik van netwerkdiensten om de toegang tot netwerkdiensten of toepassingen, waar nodig, te beperken.
d. Wanneer het van belang is dat communicatie alleen kan worden geïnitieerd vanuit een specifieke locatie of vanaf specifieke apparatuur dient automatische identificatie van apparatuur behoort te worden overwogen als methode om verbindingen van specifieke locaties en apparatuur te authenticeren.
e. Voor kritische systemen, of systemen die vertrouwelijke informatie bevatten geldt dat interactieve sessies na een vastgestelde periode van inactiviteit automatisch ontoegankelijk behoren te worden gemaakt.
f. De verbindingstijd behoort te worden beperkt als aanvullende beveiliging voor kritische systemen, of systemen die vertrouwelijke informatie bevatten.