Als alle informatie telt : een onderzoek naar kwetsbaarheden- en incidentenresponse bij ICT-organisaties

Hafkamp, W.H.M.

Publication date
2008

Begrippenlijst

Abuse
: Misbruik. Verkeerd gebruiken van een ICT-gerelateerde dienstverlening of component.

Acceptable Use Policy
: Een gedragscode voor het gebruik van de beschikbare (bedrijfs)informatie en de informatie- en communicatiemiddelen.

Alarm
: Indicatie van een schending van informatiebeveiliging of een gevaarlijke conditie die attentie behoeft.

Authenticatie
: Voorziening die ervoor zorgt dat de geclaimde identiteit van een persoon, systeem, proces of informatie wordt gewaarborgd.

Bastion host
: Een sterk beschermde computer in een netwerk dat wordt beschermd door (een deel van) een firewall waarbij het de enige computer in het netwerk is die direct kan worden benaderd via een of meer netwerken aan de andere kant van de firewall.

Beschikbaarheid
: Continuïteit; in deze context wordt bedoeld, dat gegevens binnen een redelijke tijdstermijn kunnen worden geraadpleegd of gewijzigd, wanneer dit bij het uitvoeren van werkzaamheden nodig is.

Beveiligingsincident
: Zie ICT-beveiligingsincident.

Beveiligingskwetsbaarheid
: Zie ICT-beveiligingskwetsbaarheid.

Business Continuity Management
: Het beheersen van bedrijfsrisico's teneinde een minimaal noodzakelijke productiecapaciteit en/of dienstverlening te waarborgen.

Calamiteit
: Een gebeurtenis die een service of systeem zodanig verstoort dat veelal aanzienlijke maatregelen moeten worden genomen om het originele werkingsniveau te herstellen.

Checksum
: Een berekende waarde die is gekoppeld aan de inhoud van een gegevensobject met het doel het detecteren van wijzigingen in het gegevensobject.

Classificatie
: Schema waarbij informatie wordt onderscheiden in categorieën, opdat toepasselijke informatiebeveiligingcontrols kunnen worden uitgevoerd.

Compromitteren
: Het schenden van een beveiligingsbeleid.

Computer Emergency Response Team
: Ook wel Computer Security Incident Response Team genoemd. Een organisatie waarvan de functie bestaat uit het ondersteunen van een (ICT-)gemeenschap in het voorkomen of afhandelen van aan ICT-beveiliging gerelateerde incidenten.

Configuratie-item
: De unieke naam van een hardware of softwareonderdeel of van een ICT-gerelateerd document binnen een groepering.

Constituency
: Doelgroep, bijvoorbeeld een gebruikersgemeenschap.

Cybercrime
: Computercriminaliteit; een computersysteem wordt als middel gebruikt voor het uitvoeren van strafbare feiten of een computersysteem is zelf doelwit van strafbare handelingen.

Continuïteit
: De mate waarin een computersysteem of –service ongestoord beschikbaar is.

Cryptografie
: Wiskundig proces ten behoeve van encryptie of authenticatie van informatie.

Denial of Service
: Aanval op een of meer ICT-componenten, veelal gekoppeld aan het Internet, met als doel de beschikbaarheid hiervan aan te tasten.

Defacing
: Het zonder toestemming van de eigenaar wijzigen van de inhoud en/of het aanzien van een website.

Domain Name Service
: Netwerkdienst waarbij domeinnamen worden omgezet in unieke, gerelateerde IP-nummers.

Dreiging
: Een potentieel voor het schenden van informatiebeveiliging dat ontstaat, wanneer er een omstandigheid, activiteit of gebeurtenis is die afbreuk kan doen aan de informatiebeveiliging en schade kan veroorzaken.

Encryptie
: Versleuteling, proces waarbij informatie wordt veranderd in een voor iedereen onbegrijpelijke vorm met uitzondering van houders van een specifieke cryptografische sleutel.

Exploit
: Een (computer)programma dat of techniek die gebruik maakt van een softwarekwetsbaarheid en kan worden gebruikt om de beveiliging te doorbreken of anderszins een computer aan te vallen.

Firewall
: Een software- of hardwarenetwerkcomponent die gegevensverkeer van en naar de verbonden netwerken beperkt.

Fraude
: Het plegen van strafbare feiten met het oogmerk van financieel gewin.

Hacking
: Computervredebreuk, het zonder toestemming van de eigenaar binnendringen in een geautomatiseerd werk.

Host
: Een computersysteem in een netwerk.

ICT-beveiligingsincident
: Een gebeurtenis die daadwerkelijke of potentiële negatieve effecten heeft op computer- of netwerkoperaties, resulterend in fraude, verspilling, misbruik, het compromitteren van informatie, of verlies van dan wel schade aan eigendom of informatie. Voorbeelden zijn het binnendringen van een computersysteem, exploiteren van technische kwetsbaarheden of introductie van computervirussen.

ICT-component
: Een onderdeel van een ICT-configuratie.

ICT-forensisch onderzoek
: Sporenonderzoek binnen een ICT-configuratie.

ICT-incidentenbeheer
: Ook wel incidentenmanagement genoemd. ICT-Incidentenbeheer heeft de reactieve taak (dreigende) storingen in ICT-diensten weg te nemen en ervoor te zorgen dat de gebruikers zo snel mogelijk weer aan het werk kunnen.

ICT-beveiligingskwetsbaarheid
: Een fout of zwakte in een (computer)systeemontwerp of -implementatie of –operatie, die kan worden gebruikt om het beveiligingsbeleid van het systeem te schenden.

ICT-wijziging
: Wijziging van of op een configuratie-item (CI).

Incident
: Zie ICT-beveiligingsincident.

Incidentenresponse
: Het reageren op incidenten.

Informatie
: Elk gegeven, al dan niet in elektronische vorm, geschreven op papier, gezegd tijdens een bijeenkomst, of op elk ander medium, dat door een organisatie wordt gebruikt of kan worden gebruikt om een beslissing te nemen of actie op te ondernemen.

Informatiebeveiliging
: Een stelsel van maatregelen ten behoeve van het waarborgen van de beschikbaarheid, integriteit en vertrouwelijkheid van gegevens.

Integriteit
: De correctheid en de volledigheid van informatie en informatieverwerking.

Intrusion detection
: Een mechanisme waarbij indringers op een computernetwerk of computersysteem worden gesignaleerd.

Logging
: Het vastleggen van feiten en omstandigheden uit een computerproces of –systeem.

Keys
: (Cryptografische) sleutels; waarden die worden gebruikt om een cryptografische proces te beheersen, zoals encryptie of authenticatie.

Known error
: Een ICT-gerelateerd probleem waarvoor een succesvolle diagnose is gesteld en waarvoor een workaround bekend is.

Kwetsbaarheid
: Zie ICT-beveiligingskwetsbaarheid.

Monitoren
: Het (continu) waarnemen van de activiteiten van een computersysteem of –service, alsmede het registreren van waargenomen abnormaliteiten.

Netwerk
: Een verzameling objecten voor communicatie tussen ten minste twee knooppunten van apparatuur en programmatuur, waarbij gebruik wordt gemaakt van voorgeschreven communicatieprotocollen.

Operationeel risico
: De mogelijkheid van financiële schade en/of schade aan de reputatie door tekortkomingen en zwakheden in mensen, systemen, modellen, management, procedures en controles.

Operational framework
: Stelsel van operationele procedures.

Patchen
: Het implementeren van herstelsoftware op een of meer ICT-componenten.

Pretty Good Privacy
: Een encryptiemechanisme.

Phishing
: Een vorm van fraude waarbij criminelen op een geavanceerde, elektronische wijze mensen misleiden teneinde hen te bewegen vertrouwelijke informatie vrij te geven.

PKI
: Public Key Infrastructure; een ICT-infrastructuur voor het beheren en uitwisselen van encryptiesleutels.

Risico
: De combinatie van de waarschijnlijkheid van een ongewenste gebeurtenis en de consequentie hiervan.

Risicoanalyse
: Het systematisch gebruik van informatie teneinde een of meer risico's in te schatten.

Security Patch
: Het implementeren van herstelsoftware met als doel een of meer ICT-componenten te beveiligen danwel de beveiliging te verbeteren.

Signature
: Digitale handtekening; een cryptografische transformatie van gegevens die in combinatie met een systeem voorziet in authenticatie van de verzender, integriteitswaarborg van de gegevens en onweerlegbaarheid van de ondertekenaar.

Skimming
: Het illegaal kopiëren van de magneetcodes van een magneetkaart.

Sniffer
: Programma dat (netwerk)gegevensverkeer analyseert.

Spam
: Ongewenste elektronische berichten.

Spoofing
: Een aanval waarbij een entiteit zich illegaal voordoet als, c.q. de identiteit aanneemt, van een andere entiteit.

Taxonomie
: Wetenschappelijke studie van classificatie en systematiek.

Versleuteling
: Zie Encryptie.

Vertrouwelijkheid
: Exclusiviteit; in deze context wordt bedoeld, dat informatie alleen toegankelijk is voor degenen die hiertoe geautoriseerd zijn.

Virus
: Kwaadaardig programma, dat zichzelf dupliceert, waarbij het virus is gehecht aan een gewoon programma (= drager).

Vulnerability response
: Het reageren op kwetsbaarhedeninformatie.

Vulnerability scanning
: Het periodiek verifiëren van een computersysteem of netwerkcomponent op kwetsbaarheden.

Wijziging (Change)
: Wijziging van of op een Configuration Item.

Workaround
: Een (tijdelijk) werkbare oplossing naar aanleiding van een ICT incident of known error.

Worm
: Kwaadaardig programma dat zichzelf dupliceert.