RSIV regionaal samenwerkingsverband integrale veiligheid

Definitielijst

Bot/Botnet	Een bot is een geïnfecteerde computer die op afstand, met kwade bedoelingen, bestuurd kan worden. Een botnet is een verzameling van dergelijke geïnfecteerde computers die centraal bestuurd kan worden. Botnets vormen de infrastructuur voor veel vormen van internetcriminaliteit, zoals DDoS-aanvallen
Cloud	Een op internet (de 'wolk') gebaseerd model voor systeemarchitectuur, waarbij software en opslagruimte worden aangeboden als online dienst.
Cloud computing	Cloud computing is het via een netwerk – vaak het internet – op aanvraag beschikbaar stellen van hardware, software en gegevens
Cryptocurrency	Verzamelnaam voor digitale munteenheden die cryptografische berekeningen gebruiken als echtheidskenmerk en voor transacties. De bekendste en meest gebruikte cryptocurrency is de **bitcoin**.
Cybercrime-as-a-service	Werkwijze in de ondergrondse economie waarbij criminelen zonder technische kennis gebruik kunnen maken van (betaalde) diensten van anderen om cybercrime te plegen
Darkweb	Het darkweb is een onderdeel van het deepweb. Het deepweb is het deel van het internet dat niet door zoekmachines zoals onder andere Google geïndexeerd kan worden. Het darkweb bestaat uit 'darknets' of netwerken waarbij communicatie in vertrouwen plaatsvindt. Er is speciale software noodzakelijk die de gebruiker anonimiteit moet verschaffen zoals bijvoorbeeld Tor, I2P of Freenet
Datalek	Het opzettelijk of onopzettelijk naar buiten komen van vertrouwelijke gegevens
DDoS	Bij een Distributed Denial of Service wordt een bepaalde dienst (bijvoorbeeld een website) onbereikbaar gemaakt door deze te bestoken met veel netwerkverkeer vanuit een groot aantal verschillende bronnen
Defacement	Een defacement (of bekladding) is het vervangen van een webpagina met de boodschap dat deze gehackt is, eventueel met aanvullende boodschappen van activistische, idealistische of aanstootgevende aard
Encryptie	Het versleutelen van informatie om deze onleesbaar te maken voor onbevoegden
Exploit	Software, gegevens of opeenvolging van commando's die gebruik maken van een kwetsbaarheid in software of hardware om ongewenste functies en/of gedrag te veroorzaken
Hacken	Gronddelict in veel vormen van cybercrime. Het betreft het opzettelijk en wederrechtelijk (zonder toestemming) binnendringen in een computersysteem. Hierbij moet ook worden gedacht aan e-mail accounts, social media accounts, accounts bij webshops en andere soorten accounts. Dit kan door het doorbreken van een beveiliging, door een technische ingreep (bijv. geautomatiseerd wachtwoord kraken), met behulp van valse signalen of een valse sleutel (bijv. een zelf gegenereerde toegangscode die het computersysteem activeert, of een (geldig) wachtwoord dat de persoon in kwestie niet behoort te hebben) of door het aannemen van een valse hoedanigheid (bijv. onder valse hoedanigheid ontfutselen van wachtwoord en gebruikersnaam)
High Tech Crime	High Tech Crime (HTC) omvat vormen van cybercrime met een innovatief en ondermijnend karakter. Het oppakken van deze zaken gebeurt vooral door het **Team High Tech Crime** (THTC)
Internet of Things	Het Internet of Things (IoT) is een fenomeen waarbij het internet niet alleen wordt gebruikt om gebruikers toegang te bieden tot websites, e-mail en dergelijke, maar om apparaten aan te sluiten die het internet gebruiken voor functionele communicatie
Malvertising	Het verspreiden van malware door die aan een advertentiebemiddelaar aan te bieden, zodat grote groepen gebruikers worden besmet via legitieme websites

Malware	Samentrekking van malicious software. Malware is de term die tegenwoordig als generieke aanduiding wordt gebruikt voor onder andere virussen, wormen en Trojaanse paarden
Phishing	Verzamelnaam voor digitale activiteiten die tot doel hebben persoonlijke informatie aan mensen te ontfutselen. Deze persoonlijke informatie kan worden misbruikt voor bijvoorbeeld creditcardfraude, maar ook voor identiteitsdiefstal
Ransomware	Type malware dat systemen en/of informatie daarop blokkeert en alleen tegen betaling van losgeld weer toegankelijk maakt
RAT	Een Remote Access Tool (soms Remote Access Trojan) wordt gebruikt voor het verkrijgen van toegang tot de computer van een doelwit om die op afstand te kunnen bedienen
Social engineering	Een aanvalstechniek waarbij misbruik wordt gemaakt van menselijke eigenschappen als nieuwsgierigheid, vertrouwen en hebzucht om vertrouwelijke informatie te verkrijgen of het slachtoffer een bepaalde handeling te laten verrichten
Spearphishing	Variant van phishing die zich richt op één persoon, of een zeer beperkte groep personen, die specifiek wordt uitgekozen op basis van hun toegangspositie om een zo groot mogelijk effect te sorteren zonder al te veel op te vallen

Lijst met afkortingen

RBO	Regionaal Bestuurlijk Overleg
NCTV	Nationaal Coördinator Terrorismebestrijding en Veiligheid
NCSC	Nationaal Cyber Security Center
CERT	Computer Emergency Response Teams
DTC	Digital Trust Center
MKB	Midden- en Klein Bedrijf
AP	Autoriteit Persoonsgegevens
GFCE	Global Forum on Cyber Expertise
GCCC	Global Counsil of City CIO's
CIO	Chief Information Officer
HSD	The Hague Security Delta (HSD)
ICT	Informatie en Communicatie Technologie
LMIO	Landelijk Meldpunt Internet Oplichting
CBS	Centraal Bureau voor de Statistiek
CISO	Chief/Corporate Information Security Officer
IBD	Informatie Beveiligings Dienst
BIG	Baseline Informatiebeveiliging Gemeenten
AVG	Algemene Verordening Gegevensbescherming
VNG	Vereniging Nederlandse Gemeenten
CCV	Centrum voor Criminaliteitspreventie en Veiligheid