Digitale criminaliteit

ICT en andere digitale processen zijn tegenwoordig onlosmakelijk verbonden met bedrijven. Het toenemende gebruik van netwerken met een open verbinding met het internet, maar ook de anonimiteit en brede bereik van het internet, biedt echter ook uitgelezen kansen voor High Tech Crime; criminaliteit waarbij ICT als middel wordt ingezet. Reden des te meer om uzelf als ondernemer maar ook uw medewerkers op de hoogte te houden van de ontwikkelingen.

Cybercriminaliteit

Onder High Tech Crime vallen verschillende soorten van criminaliteit. Deze activiteiten zijn ruwweg in twee verschillende categorieën te verdelen: cybercriminaliteit en computercriminaliteit. Criminele activiteiten die gericht zijn tegen personen, eigendommen en organisaties (waarbij ICT dus als middel wordt ingezet) zijn bekend onder de noemer cybercriminaliteit. Deze traditionele delicten kunnen ook zonder tussenkomst van ICT gepleegd worden, maar hebben door het gebruik van ICT een nieuwe (efficiëntere) uitvoering gekregen. Door het gebruik van innovatieve technieken kan ICT bijvoorbeeld als communicatiemiddel worden ingezet waarbij de communicatie zelf kan worden afgeschermd voor onbevoegden (waaronder de opsporing). Deze technieken variëren van slimme vindingen (zoals het voortdurend wisselen van niet-geregistreerde mobiele telefoons of het gebruik van 'dead letter boxes' waarbij concept- e-mailberichten door meerdere gebruikers kunnen worden ingezien en aangepast zonder dat berichten daadwerkelijk worden verzonden) tot geavanceerde technieken als encryptie (waarbij de inhoud van berichten wordt versleuteld met codes) en steganografie (waarbij het hele bestaan van een bericht wordt verhuld door deze bijvoorbeeld in een afbeelding of digitale clip te verwerken). Naast communicatie wordt ICT ook als handelskanaal ingezet voor illegale goederen en diensten. Bekend zijn de spam-berichten met geneesmiddelen en merkvervalste producten, maar ook wapens, drugs, kinderporno en mensenhandel worden via internet aangeboden.

Internetfraude

Naast communicatie en handel richt cybercriminaliteit zich ook op financieel-economische criminaliteit, waaronder fraude, oplichting en bedrog. Ook het op een slinkse wijze vertrouwelijke informatie verkrijgen (identiteitsfraude) waarmee vervolgens bank- en creditcardfraude kan worden gepleegd komt veel voor. Internetfraude kent een diversiteit aan werkwijzen en technieken zoals phishing (verkrijgen van informatie via een vervalste website), spamming, malware en pharming (verkrijgen van informatie via een doorlink naar een andere server).

> 'Naast fraude kan ICT ook worden gebruikt om boodschappen van illegale inhoud te verspreiden'

Afpersing en chantage is vaak gerelateerd aan het hacken van systemen en het dreigen met (distributed) Denial of Service of (d)DoS-aanval (het bewust verzenden van massale hoeveelheden gegevens naar systemen waardoor deze overbelast raken en onbereikbaar worden).
Naast fraude kan ICT ook worden gebruikt om boodschappen van illegale inhoud te verspreiden. De publieke moraal of de persoonlijke levenssfeer van slachtoffers worden daadwerkelijk met deze activiteiten aangetast. Voorbeelden hiervan zijn haat zaaien via discussiefora en chatboxen. Van illegale communicatie is ook sprake wanneer zonder toestemming computer- en telefoongegevens van derden ongemerkt worden onderschept (spionage). Daarvoor worden methoden en middelen ingezet als hacking, spyware (ongemerkt op de computer geïnstalleerde software die gegevens verzamelt en doorstuurt naar een derde partij) en malware. Ook keyloggers (waarbij toetsaanslagen en muisklikken worden doorgestuurd naar een derde partij) kunnen voor deze illegale doeleinden worden ingezet.

Computercriminaliteit

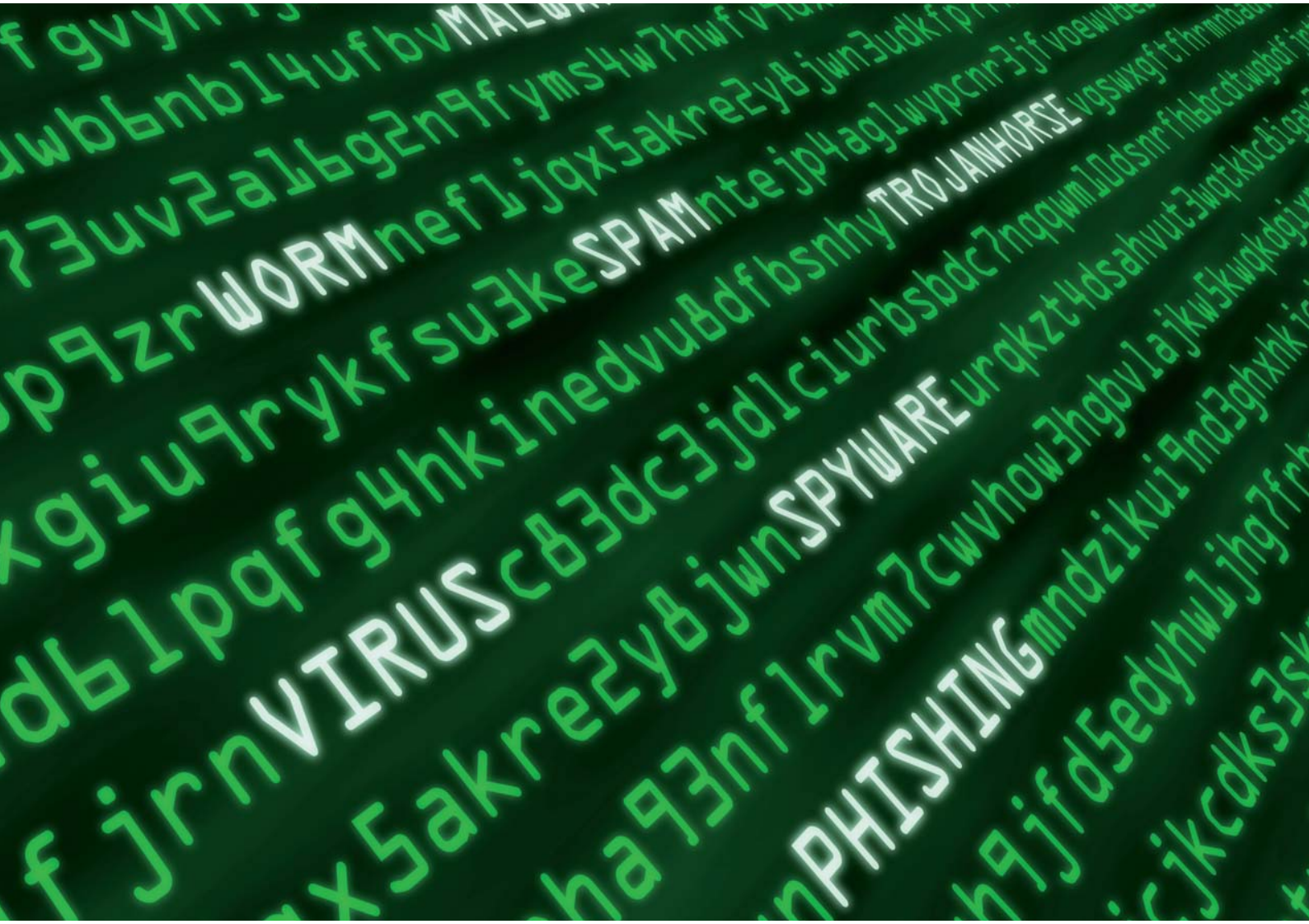
Activiteiten gericht op elektronische communicatienetwerken en informatiesystemen (waarbij ICT zowel middel als doelwit is) behoren tot de groep computercriminaliteit. Deze vorm van criminaliteit kan dus niet bestaan zonder ICT. In de meeste gevallen gaat het om het inbreken, verstoren, manipuleren of wijzigen van systemen dan wel om het ontwikkelen en voorzien van instrumentele middelen die hierbij helpen. Een van de meest bekende voorbeelden is het ongeautoriseerd toegang verschaffen tot ICT, wat door de zogenaamde hackers wordt gedaan. Zij beschikken over een grote mate van expertise en technische kennis en kunnen hiermee inbreken op (beveiligde) systemen, instrumenten ontwikke-

len om ICT-storingen mee te veroorzaken. Eén van de belangrijkste criminele instrumenten die door hackers kunnen worden opgezet zijn botnets. Dit zijn verzamelingen van op afstand bestuurbare computers die instrumenteel zijn voor het plegen van diverse varianten van high-tech crime, vooral spamming, phishing en (afpersing met behulp van) (d)DoS-aanvallen.
Naast in inbreken op systemen kan ook de werking van de systemen (bijvoorbeeld websites, e-maildiensten of computernetwerken) op verschillende manieren worden verstoord. Twee belangrijke varianten die wereldwijd enorm zijn toegenomen zijn (d)DoS-aanvallen en spamming. Bij spamming kunnen ook storingen worden veroorzaakt door het versturen van massale e-mails, maar dit is eerder een neveneffect van digitale marketing en reclame dan een concreet doel.

Storingen kunnen ook direct worden veroorzaakt door het daadwerkelijk manipuleren (beschadigen, verwijderen, wijzigen of vernietigen) van gegevens en systemen. Malware is het bulkbegrip voor dubieuze computerprogramma's die zonder toestemming van de eigenaar of beheerder draaien op een computer en het systeem iets laten doen naar de wens van een buitenstaander. Dergelijke programma's worden door specialisten op maat gemaakt en kunnen ongemerkt vertrouwelijke informatie van gebruikers verzamelen, data en systemen beschadigen (de bekende virussen), of externe toegang verlenen op computers (via de moderne virussen, zogenoemde Trojaanse paarden). Ook complete websites kunnen worden geblokkeerd of gewijzigd (defacing), onder meer als instrument om mensen mee op te lichten (bijvoorbeeld internetfraude door middel van nepwebsites), af te persen, of om uiting te geven aan protest (hacktivisme).

Zoek de zwakke plekken

High Tech Crime is enkel en alleen mogelijk wanneer derden met criminele intenties toegang krijgen tot uw computernetwerk. Door zwakke plekken binnen



de ICT-infrastructuur te analyseren en aan te pakken kunt u het de daders in ieder geval moeilijker maken.
Een eerste zwakke plek is de internetverbinding. In Nederland is een hoge ADSL-dichtheid aanwezig, waarbij computers vrijwel permanent in verbinding staan met het internet. Dit maakt ons land een zeer aantrekkelijk werkterrein voor onder andere phishers. Toegang tot computers via uw netwerk kan worden bemoeilijkt door goede anti-virus software zoals een virusscanner en firewalls te installeren en deze regelmatig te controleren op werking, updates en eventuele lekken. Het instellen en regelmatig veranderen van wachtwoorden maakt de toegang voor partijen en slechte bedoelingen eveneens moeilijker. Denk daarbij ook aan het gebruik van laptops, iPads en smartphones. En natuurlijk moeten de medewerkers die regelmatig thuis werken ook voorzien zijn van goed beveiligde apparatuur.

Een tweede risicofactor zijn de medewerkers van een bedrijf. Wanneer zij onzorgvuldig met veiligheidsmaatregelen omgaan, loopt het ICT-netwerk een groter risico. Het onzorgvuldig omgaan met veiligheidsmaatregelen en bedrijfsgeheimen kan door middel van voorlichting en beveiliging van bedrijfssystemen worden tegengegaan.
Een medewerker kan het netwerk ook doelbewust blokkeren of ontregelen Het doelbewust saboteren van de digitale infrastructuur kan vanwege corruptie, maar ook uit wraak (bijvoorbeeld van een exwerknemer) worden gedaan. Daarnaast huren bedrijven ook steeds vaker IT-consultants extern in om systemen of software te bouwen. Wanneer dit mensen zijn met criminele bedoelingen of wanneer criminelen als zelfstandige ondernemers ICT-diensten op de markt aanbieden, kan er sprake van een aanmerkelijk veiligheidsrisico. Een goede screening van personeel en derden, oplettendheid bij afwijkend gedrag van medewerkers en het opleiden en behouden van eigen IT-personeel kan interne oorzaken van ICT-leed voorkomen.

Deel kennis

High Tech Crime is een fenomeen waar uw onderneming lastig tegen te wapenen is. Preventie en een pro-actief beleid kan echter veel schade voorkomen. Een belangrijke stap daarin is dat uw ICT-beheerder op de hoogte blijft van de ontwikkelingen op het gebied van ICT en de daarmee gepaard gaande mogelijkheden voor criminelen. Door deze ontwikkelingen om te zetten in een preventiebeleid met duidelijke voorzorgsmaatregelen voor de rest van uw medewerkers betrekt u hen actief bij het proces en houdt u hen ook op de hoogte.

Bron: High Tech Crime, soorten criminaliteit en hun daders. Literatuurinventarisatie van het WODC