CYBER ANNO 2012

Mevrouw Petra van Schayik, Compumatica

CYBER. Eén woord met vele betekenissen: ongrijpbaar, een hype en bijzonder vervelend.
Cyberaanvallen zijn virtuele ongrijpbare bedreigingen die 24 uur per dag aanwezig zijn en geen rekening houden met landsgrenzen, bedrijven en of personen.

OVER DE AUTEUR

Mevrouw Petra van Schayik is Managing Director van Compumatica secure networks BV en van Compumatica secure networks GmbH.

www.compumatica.eu

CYBERAANVALLEN

Het aanvalsrisico wordt enerzijds bepaald door het land waarin je leeft, de aard van de organisatie, bedrijfsprocessen en/of het bedrijf, maar anderzijds is iedereen die verbonden is met of actief is op het World Wide Net een potentieel slachtoffer.
Nieuw is het niet, het komt al sinds de jaren 90 voor, de bekendheid heeft het gekregen doordat de media zich er massaal op gestort hebben en het tot hype hebben verklaard. Vele praatshows, rubrieken en tijdschriften worden er mee gevuld. Welwillend werken deskundigen en zogenaamde deskundigen hieraan mee. Enkele Nederlandse incidenten hebben zelfs de wereldpers gehaald.
Cyber is echter niets meer dan crimineel gedrag met het doel het slachtoffer zoveel mogelijk schade toe te brengen om persoonlijk gewin te boeken of het ontwrichten van de maatschappij. Het kan zijn een inbraak in een netwerk van een land of concurrent, zonder dit te melden, om zoveel mogelijk informatie te verkrijgen. Deze informatie wordt dan gebruikt om commercieel voordeel te halen of te verkopen aan de hoogst biedende.
Een ander doel is de inbraak in een netwerk en dit aan de betreffende organisatie te melden om deze daarna af te persen. Weer andere inbraken leveren direct een geldvoordeel op door financiële transacties te manipuleren.

DOORDACHTE BESCHERMING EN BEWUSTWORDING

De bescherming bij Cyber moet liggen in het kweken van bewustwording bij de gebruiker en het toepassen van beschermingsmaatregelen. Voor organisaties is het belangrijk om een aansluitbeleid vast te stellen. Op welke manier koppel je systemen en netwerken aan elkaar? Welke beveiligingsmaatregelen pas je zelf toe op de computersystemen, netwerken en firewalls en wat eis je van je communicatie partners?

Het nieuwe werken verhoogt mijns inziens het dreigingniveau voor het de centrale organisaties doordat er vanaf "elke" plek gewerkt kan worden.

Niet te vergeten in cyber is "Cloud Computing", allerlei informatie wordt ergens opgeslagen en gebruikers hebben wereldwijd toegang tot de Cloud. Dit kan gebeuren door een open wifi verbinding op een vliegveld of een sessie in een internet café. Het is voor de eigenaar van de data niet altijd duidelijk waar de gebruiker zit. Ook moet hij vertrouwen op de infrastructuur van de dienstverlener. De Cloud biedt voor de cybercrimineel een nog onontgonnen gebied met veel perspectief.

Het belangrijkste bij cyber is enerzijds dat je er weet van hebt dat de dreiging toeneemt en dat je voldoende beschermingsmaatregelen neemt ten aanzien van de eigen infrastructuur en data. Daarnaast moet je er voor zorgen dat de medewerkers bewust zijn van de risico's. Cyberkennis en bescherming moeten een standaardonderdeel worden van de introductie van nieuwe medewerkers. Voor alle bestaande medewerkers moet er een bewustwordingstraining gestart worden. Daarnaast pleit ik ervoor dat we cyberbewustwording en voorkoming als leerdoel in het onderwijs opnemen.
Een online cybertraining voor alle internet gebruikers via een postbus 51 website met een promotiecampagne kan ervoor zorgen dat iedereen op de hoogte is van de risico's en veilig surft.

ROL PROVIDERS

Volgens mij hoort het aanbieden van "schone content" tot een taak van de providers. Dit kan bestaan uit goede antivirus software op niveau van de provider, het inzetten van "intrusion detection and prevention" systemen. Hierdoor kunnen spam en virussen op centraal niveau gewist worden. Dit is enerzijds tegenstrijdig met de vrijheid op internet anderzijds zit niemand te wachten op spam en virussen. De providers kunnen de kosten hiervan meenemen in hun contracten.

ROL OVERHEID

De overheid moet samen met de vitale infrastructuur en de security leveranciers een duidelijk plan opstellen ter bescherming van haar vitale infrastructuur en content.
Belangrijk daarbij is te weten waar de belangrijkste cyberdreigingen vandaan komen. Voor onze overheid kunnen dit wisselende landen zijn, afhankelijk van politieke en/of militaire activiteiten.

CYBER TERRORISME

Cyber terrorisme wordt een steeds sterker fenomeen, door de verregaande fysieke beschermingsmaatregelen wordt het steeds moeilijker daadwerkelijk doelen aan te vallen. De cyberterrorist kan veilig achter zijn computersysteem de grootst mogelijke aanslagen plegen zonder dat de groepering te achterhalen is.
Door een gerichte cyberaanval kan een land of een deel van een land in totale chaos geraken. Je hoeft in de Randstad maar te denken aan het uitschakelen van de elektriciteit, het mobiele telefoonnetwerk en de wegsignalering en de chaos is compleet. De impact hiervan is niet voor te stellen. Enkele miljoenen mensen kunnen niet meer werken, communiceren en daarnaast is het verkeer compleet ontregeld. Onbekend bij een dergelijk aanval is hoe lang zal deze duren, wanneer zijn alle systemen weer actief etc.

CYBERPOLITIE EN CYBERLEGER

Een dergelijk scenario geeft aan dat je dit als Nederland niet alleen kunt, er zal internationaal samengewerkt dienen te worden. Een cyberpolitie en een cyberleger is noodzakelijk, enerzijds om cyberaanvallen proberen te voorkomen en daarnaast om bescherming te bieden. Verregaande Nederlandse, Europese en mogelijk wereldwijde wetgeving is nodig om cyberaanvallen en cyberterrorisme het hoofd te bieden. Uitgangspunt moet hierbij zijn dat er snel met een korte responstijd opgetreden kan worden in urgente situaties.
De vraag of je als politie of land een cyberaanval moet beantwoorden met een cyberaanval op de aanvaller is mijns inziens zeer discutabel. In de reële wereld is dit immers niet gebruikelijk, in het bijzonder bij het overschrijden van de landsgrenzen.

SAMENWERKING OVERHEID EN INDUSTRIE

Samenvattend Cyber kan men van vele kanten benaderen en er is een noodzakelijkheid om als overheid samen met de industrie tot oplossingen te komen om ervoor te zorgen dat de digitale wereld zo veilig mogelijk wordt.