0THEMA10CYBER00010C0101100Y1010B0101E00110R01TH01E01M001A1CY1010B00001B1100010ER10010100

LATEN WE STOPPEN MET BESTRIJDEN CYBERCRIME!

De heren Ronald Prins (CEO en oprichter Fox-IT) en Joost Bijl (Marketing Manager), Fox-IT

We bestrijden cybercrime al geruime tijd. Als je terug kijkt in het recente verleden lijkt dit vrij succesvol te zijn. Is dat ook zo?

Waarom moeten we stoppen met het bestrijden van cybercrime? In de wiskunde wordt gewerkt met normen. Normen zeggen iets over bijvoorbeeld een lengte of grootte. In de echte wereld wordt ook met normen gewerkt, bijvoorbeeld in het verkeer. Zo kan de wet een andere norm voor een veilige snelheid hanteren als ik. Als ik te snel rij volgens de politieman met lasergun raak ik mijn rijbewijs kwijt. Iedereen houd er andere normen op na, niet alleen in wiskunde of het verkeer maar ook in cyberspace.

In cyberspace is het bepalen van de norm echter nog niet zo eenvoudig. Er is niemand met een laser gun en de maximum snelheid is ook niet bekend. Het is onontgonnen terrein voor de gebruikers en de handhavers. ***Zodra we de normen hebben opgesteld is het weer tijd om cybercrime te gaan bestrijden.***

We hebben het succes van het Bredolab. Hierbij is een Armenische verdachte opgepakt voor het besmetten van 30 miljoen computers. Hij verkocht de besmette computers aan andere criminelen die het vooral gebruikten om uiteindelijk bankrekeningen te plunderen of spam te versturen. Zijn inkomen was al gauw 1 miljoen US Dollar per maand. Het oppakken van deze verdachte was niet eenvoudig maar gelukkig maakt hij wat fouten.

Een tweede "succes" is de aanpak van kinderporno op servers die zich schuil hielden in het Tor-netwerk. De enige manier, technisch gezien, om deze mensen te stoppen was door in te breken op hun computers. Eenmaal binnen zijn de afbeeldingen vervangen door het logo van de politie. Een succesverhaal, niet alleen vanwege het directe effect maar ook vanwege de afschrikkende werking.

Halverwege november liet de Vereniging van Nederlandse banken weten dat de cybercrime gerelateerde fraude was verdubbeld. Fox-IT beschermt een aantal Nederlandse banken tegen fraude bij online bankieren en stopt iedere maand meer fraude dan de maand daarvoor. ***Beide kampen vieren hun successen.***

Bovenstaande voorbeelden geven ons het gevoel dat we goed bezig zijn in de aanpak van cybercrime. We moeten niet vergeten dat de tegenstanders ook grote stappen maken. Cyberspace is een droomplaats voor criminelen. Je kunt eenvoudig inbreken en de kans dat je gepakt wordt is nog niet heel hoog. Het is tijd voor een pas op de plaats en goed na te denken over de volgende stap.

ICT-Journalist Brenno de Winter heeft met 'Lektober' aangetoond hoe simpel het is om een datalek te vinden. Elke dag in oktober werd een kwetsbaarheid in een, vaak bekende, website bekend gemaakt. Sommige van deze getroffen sites hebben wij achteraf onderzocht.

Het moge duidelijk zijn dat er technisch iets mis was met deze sites. Veelal waren basismaatregelen niet aanwezig. Misschien nog beangstigender is de houding van de getroffen organisaties. Vaak waren ze al uitgebreid onderworpen aan een audit. Respectabele bedrijven hebben allerlei vooraf afgesproken zaken als de password policy gecontroleerd. Niet zelden werden hierbij basale dingen over het hoofd gezien, zoals het gebruik van standaard wachtwoorden voor de systeembeheerder

Gelukkig waren sommige audits wel van voldoende kwaliteit. Toch zijn de resultaten van die audits niet doorgevoerd. De aangedragen redenen hiervoor zijn dat het te duur was, het rapport onbegrijpelijk of dat een teruggezette back-up de maatregelen ongedaan had gemaakt.
Hoe moet dit probleem worden opgelost? Een vaak gehoord argument is dat 100% veiligheid niet bestaat. Dat klopt, maar 95% is misschien wel mogelijk. Het veiligheidsniveau van sommige Lektober-sites was echter ver beneden pijl, zeg 10%. Hier valt dus veel te winnen.

Een aantal voor de hand liggende manieren om dit beveiligingsniveau op te krikken zijn.

- **Security by design:** Je kunt beveiliging niet achteraf 'er bij' doen, dit moet je vanaf het begin mee ontwerpen. Aan het begin van een project heb je nog de kans de juiste keuzes te maken en is er nog budget beschikbaar.
- **Kennis over beveiliging** is nog niet overal adequaat genoeg. Analyse van Lektober incidenten laat zien dat programmeurs vaak basiselementen zoals 'input validation' vergeten. Het kost 5 minuten om uit te leggen, waarom wordt het dan niet gedaan?

- **Focus:** Security en business continuity staan vaak op gespannen voet met elkaar. Het is dan ook niet handig om deze twee functies in 1 persoon te verenigen.
- **Balans:** Richt je niet alleen op preventieve maatregelen maar tref ook detectieve maatregelen. Systemen zijn misschien niet 100% dicht te timmeren, maar we kunnen vaak nog wel detecteren dat een hacker aanwezig is. Investeer in Intrusion Detection Systemen of neem hiervoor een dienst af.

Bovenstaand lijstje is niet nieuw en kan iedere beveiligingsexpert verzinnen of verbeteren. ***De echte vraag is waarom het niet gebeurt!***

Reden 1 – Bewustwording. Misschien heeft de Diginotar-case ogen geopend. Ministers hebben nachten moeten doorhalen vanwege een gehacked bedrijf. Ondertussen wordt cybersecurity regelmatig besproken in het parlement.

Reden 2 – Geld. Als we meer bewust waren van de gevaren zouden we er misschien ook meer aan uitgeven. ***Ten tijde van economische crisis en korte termijn prikkels zoals bonussen wordt al snel bezuinigd op beveiliging.***

Reden 3 – Security is niet zelfde als Compliancy. Veel organisaties stellen vertrouwen in keurmerken, audits of andere vormen van compliancy. ***Het is niet zo dat een jaarlijkse audit je beschermt tegen werkelijke beveiligingsrisico's***, vaak hebben ze zelfs weinig met elkaar te maken. En je zou kunnen stellen dat ze vaak een vals gevoel van veiligheid geven. Kortom de audit heeft tot effect dat de werkelijke security achteruit gaat.

De oplossing voor reden 1, 2 en 3 is dat de overheid het initiatief moet nemen. Er is geen tijd om te wachten totdat 'de verantwoordelijken' het licht zien.

Eerder genoemde voorbeelden betroffen cybercrime en direct financieel verlies. In de huidige samenleving, waar alles met elkaar verbonden is, zijn er grotere zorgen. Virussen kunnen energiecentrales uitschakelen en onlangs is een artikel verschenen waarin iemand beweerde het netwerk van een Boeing 747 over te kunnen nemen vanuit een passagiersstoel.

Wat moet de overheid doen?

Ten eerste moeten de juiste economische stimulansen wordt geïntroduceerd. Bedrijven moeten het financieel merken als hun beveiliging faalt. Dit principe gebruikt de USA om banken te straffen die vergeten betalingen aan terroristen te blokkeren of om omkoping af te straffen. Hierbij stuur je dus op resultaat. Financiële motieven overtuigen beslissers als geen ander, in het bijzonder in een commerciële organisatie.

Ten tweede moet er actief hulp worden geboden. Voor de meeste vitale zaken zoals de energiesector, vliegleiding, ziekenhuizen en nucleaire installaties zou de overheid actief moeten helpen. Ze hoeven geen werk uit handen te nemen maar bijvoorbeeld een oogje in het zeil houden op internet. Hiervoor moet wel goede wetgeving worden opgesteld om privacy te waarborgen. De overheid kan dan bijvoorbeeld grootschalige virus aanvallen of spionage detecteren.

Ten derde moet de handhaving op cyberspace machtsmiddelen krijgen. In de echte wereld draagt de politieman een wapen, in cyberspace is iedereen gelijk. Het is haast onmogelijk om criminelen te arresteren die in land A wonen en geld stelen in land B via servers in land C. Uiteraard is hiervoor samenwerking op allerlei niveaus voor nodig zoals EU, NAVO en UN. Dit staat niet in de weg om hier alvast op nationaal niveau mee te beginnen.

Als we bovenstaande zaken geregeld hebben is het weer tijd om de strijd met cybercrime aan te gaan. ***"You can win a battle but still lose a war."***

0THEMA10CYBER0010C01011000Y1010B0101E0011OR01TH01E01M001A1CY1010B00001B1100010ER10010100