THINKSECURE

“Security Starts With Awareness”

Think Secure

Think Secure is in 2003 opgericht met het doel organisaties te ondersteunen met kennis en diensten die:

1. Het bewustzijn m.b.t. informatie- en ICT beveiliging tot een hoger niveau te helpen tillen met de daarbij behorende processen en oplossingen
2. De ICT en informatie infrastructuur beveiligen. Dit bewerkstelligen wij door audits, kwetsbaarheid analyses, quick scans en penetratie testen uit te voeren bij onze klanten
3. Een grondig advies te geven op basis van de bevindingen. Dit kan zowel op organisatie, infrastructuur, proces- en product niveau worden gegeven.
4. Onafhankelijk opereren ten opzicht van oplossingen. Wij leveren geen technologische oplossingen, maar werken wel samen met vendors en partners die op dit gebied actief zijn.

Think Secure’s motto “security starts with awareness” geeft aan waarvan wij zijn overtuigd, “het beveiligen van ICT informatie en informatie begint met gezond verstand en het bewustzijn hoe de zaken er voor staan en er aan blijven werken om een acceptabel en beheersbaar niveau van beveiliging te behouden”.

Think Secure

Think Secure werk strategisch samen met een aantal partners. Deze partners zijn gespecialiseerd in een aantal waarde toevoegende disciplines waaronder:

- Bedrijfsrecherche
- Fraude onderzoek
- Cyber forensics
- Product oplossingen
- Risc Management en incident bestrijding
- Anti- terrorisme, E-Espionage en anti cybercrime

Security incidenten: een dagelijks feit

SECURITY

'Bedrijven bezuinigen op beveiliging'

Microsoft-fix voor IE-lek werkt onvoldoende

SECURITY
Jolein de Rooij

De snelle fix die Microsoft vorige week uitbracht voor een ernstig lek in versies 6 en 7 van Internet Explorer, werkt volgens Govcert niet in alle gevallen. Het computerincident-responsteam van de Nederlandse overheid adviseert organisaties voorlopig niet om te stoppen met het gebruik van de browser, zoals Franse en Duitse pendanten dat dit weekend wel deden. Govcert wacht met waarschuwen totdat Microsoft een patch van voldoende kwaliteit uitbrengt. Hackers zouden het lek volgens Google misbruikt hebben in een recente aanval op Google in China en op andere bedrijven.

Microsoft spreekt tegen dat het onveilig zou zijn om Internet Explorer te gebruiken. Het bedrijf adviseert om een fix voor Internet Explorer 6 en 7 te installeren, of anders over te stappen op versie 8 van Internet Explorer. 'We hebben de fix maandag getest, maar hij werkt niet in alle gevallen. Daarom hebben we besloten nog geen waarschuwing uit te brengen,' zegt Govcert-woordvoerder Ella Broos. Govcert wil ook niet adviseren om te stoppen met het gebruik van Internet Explorer, zoals Duitse en Franse pendanten van het computerincident-responsteam dat wel hebben gedaan. 'Dat is nogal wat. We zien nog geen misbruik van het lek en wachten daarom met waarschuwen totdat Microsoft een patch komt die afdoende is

Govcert wil extra beveiliging GSM-verkeer

MOBILITY
Jolein de Rooij

'Partijen als netwerkoperators, leveranciers van mobiele apparaten en banken moeten zelf het initiatief nemen om het gsm-verkeer extra te beveiligen.

Het duurt geen jaren meer voordat de eerste gerichte aanval op een sms-authenticatiedienst plaats kan vinden.' Dat zegt Ton Slewe, adviseur bij Govcert.Het computerincident-responsteam van de Nederlandse overheid adviseert om vertrouwelijke telefoongesprekken niet meer over gsm te laten verlopen.

Steeds meer malware via mobieltjes

Ruim tweehonderd personen reageerden op de per e-mail verstuurde uitnodiging om een vragenlijst in te vullen.

Buiten roken bedreigt IT

Het antirookbeleid heeft een onverwachte uitwerking op IT-beveiliging. Het blijkt nieuwe risico's op

Algoritme vernietigt zoekprofielen websurfer

Computer berekent 3D-model van gezichten

Gekraakte iPhone is riskant bij bankieren

Door een onzer redacteuren

ROTTERDAM, 24 NOV. De Apple iPhone wordt ook door hackers serieus genomen. ING maakte gisteren bekend dat bezitters van een gekraakte ('jailbreaked') iPhone het risico lopen dat hun bankgegevens in verkeerde han-

OpenSSH wordt telkens geïnstalleerd met hetzelfde wachtwoord. Wie dat niet veranderd heeft en de afgelopen dagen inlogde op de ING-site, loopt kans slachtoffer te zijn.

Apple heeft zijn smartphone dichtgespijkerd, bijvoorbeeld om

in de respons van de zoekmachine. Zo is nogal wat extra netwerkverkeer nodig voor het antwoord belandt op de vragende computer. Verder introduceert de client vertraging door het versleutelen van het verkeer tussen de clients onderling en met de centrale server.

Dat de centrale server steeds moet wachten tot een groep compleet is, is volgens projectleider Alexandre Viejo van de afdeling Computer Engineering van de Rovira i Virgili University niet zo'n probleem. Het protocol is immers bedoeld om de werking van het profielalgoritme van de zoekmachine te frustreren. Dat betekent niet dat een websurfer niet af en toe een vraag direct kan stellen wanneer de server te lang doet over het formeren van een groep. Een teller in de client houdt bij of het aantal direct gestelde

Gereedschap gericht op herstel privacybescherming

Een UMTS-antenne op het Europlatform 60 kilometer in zee blijkt voor de Rotterdamse haven een

UMTS-dekking op zee biedt extra veiligheid

De beveiliging van

We investeren ons suf in firewalls, virusscanners, inbraakdetectiesystemen en peperdure securityconsultants. Dat alles om onze infrastructuren, processen en gegevens te beschermen. Ondertussen lopen onze medewerkers elke dag met memory sticks, dvd'tjes, draagbare schijven en complete laptops vol gevoelige data het bedrijf in en uit. Dat gaat maar al te vaak mis: sticks,

f gestolen, en laptops kunnen worden misbruikt om via het VPN het bedrijfsnetwerk binnen te dringen. AAD OFFERMAN

Indringers verklik

Hoe herkent u misbruik en welke maatregelen kun

Als u programma's gebruikt om het verkeer op uw internetverbinding in de gaten te houden, dan stuit u misschien op pogingen tot misbruik. Ook op andere manieren kunt u ontdekken dat er iets mis is. Gelukkig staat u er niet alleen voor: providers helpen doorgaans graag om hackers, spammers of verspreiders van virussen op te sporen en aan te pakken. Maar hoe benadert u ze? Wie moet u hebben? En waar moet u op letten bij het indienen van een klacht?

'Beveiliging creditcardtransacties onder de maat'

Protocol van Visa en Mastercard afgeserveerd

Hoog tijd dat de wetgever in actie komt om de consument te beschermen

Automatisering Gids

E-spion heeft hier vrij spel

AIVD brengt brochure uit als waarschuwing tegen digitale spionage

Spam-wet verlaagt drempel e-spookfactuur

ECM
Anneke Houtman

Statistieken: een moment opname

- ✓ De energie en olie sector zien een explosieve groei van 356%, de pharma en chemie sector een groei van 322% en andere sectoren een groei van 252% van Trojan gerelateerde data diefstal (bron: Scansafe)
- ✓ AIVD brengt brochure uit om bedrijven tegen E-spionage te waarschuwen
- ✓ In een recentelijke survey bleek dat 84% van de ondervraagde organisatie minimaal 1 inbraak met als gevolg data lekkage heeft ondervonden, 44% van de ondervraagde bedrijven hadden tussen 2 en 5 inbraken gehad.
- ✓ Van de ondervraagden beantwoorden 83% de vraag wat de belangrijkste focus was m.b.t. Security doelen binnden de organisatie met "het toenemen van de focus op informatiebeveiliging (bron Trial by fire, PWC 2010)
- ✓ 36% van alle data lekkage/diefstal in de survey bestond incidenten met laptop of devices met opslagcapaciteit. (bron: Ponemon)
- ✓ 56% van de incidenten die via het web hebben plaatsgevonden zijn PDF gerelateerd
- ✓ Respondents reported big jumps in incidence of password sniffing, financial fraud, and malware infection. (bron: CSI Computer Crime and Security Survey 2009)
- ✓ In 2009 had 72% van de ondervraagden van een Erst & Young survey geen vertrouwen in Justitie voor wat betreft cybercrime bestrijding. Dit verklaarde ook het feit dat weinig organisaties aangifte doen van misdaden die met Cybercrime te maken hebben.
- ✓ Volgens een onderzoeksrapport van de Universiteit van Bedfordshire is 62% van de aanvallen van gemiddelde geraffineerfdheid. Er was niet veel nodig om zich toegang te verschaffen tot de doelen.

Think Secure Diensten

- ✓ Kwetsbaarheid Analyses
- ✓ Webapplicatie kwetsbaarheid testen
- ✓ Penetratie testing
- ✓ Security, IT audits en nulmetingen
- ✓ Trainingen mb.t. kwetsbaarheid analyse en awareness
- ✓ Social Engineering
- ✓ Het ontwikkelen van beleid, policy en procedures
- ✓ ISO, SOX en andere projecten die te maken hebben met certificatie
- ✓ Project ondersteuning in projecten waar informatiebeveiliging een belangrijke rol speelt
- ✓ Interim management voor security functies
- ✓ Consultancy
- ✓ Digitaal Forensisch onderzoek

In welke sectoren zijn wij actief

Onze klanten bevinden zich o.a. de volgende sectoren:

☐ Financiële instellingen
☐ Petro- en chemische sector
☐ Energiebedrijven
☐ Lokale overheid
☐ Landbouw
☐ Industrie
☐ M.K.B.

THINKSECURE