



“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
- Risk Management en incident bestrijding
- Anti- terrorisme, E-Espionage en anti cybercrime



Security incidenten: een dagelijks feit



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 om een fix voor Internet Explorer 6 en 7 te installeren, of anderszels te

Fransen en Duitse pendanten dat dit weekend wel deden. Govcert wacht met waarschuwen totdat Microsoft een patch van voldoende kwaliteit uitgeeft. 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 anderszels te

stoppen op versie 6 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-voorzitter 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

SECURITY

'Bedrijven bezuinigen op beveiliging'

Partijen als netwerkers, leveranciers van mobiele apparaten en banken moeten zelf initiatief nemen om de hun-veerker extra te beveiligen. Het duurt geen jaren meer voordat de eerste gerichte aanval op een sms-authenticatielid plaats kan vinden. Dat zegt Ton Siewe, adviseur bij Govcert. Het computerincident-responsteam van de Nederlandse overheid adviseert om vertrouwelijke telefoongesprekken niet meer over gsm te laten verlopen. Ook nieuw bij aanvullende van smartphones.

Govcert wil extra beveiliging GSM-verkeer

Publiek misbruik van het gsm-protocol is volgens Govcert dichtbij gekomen, nu onderzoeker Karsten Nohl in december aantoonde dat berichten en telefoongesprekken kunnen worden ontleend. Dat betekent in principe ook dat bewijzenden de codes die banken via sms aan hun klanten sturen om er online transacties mee te kunnen bevestigen, in de toekomst kunnen afuitsturen. Hooftel volgens Siewe geen jaren meer duurt voordat de eerste gerichte aanval op een smartphone

Steeds meer malware via mobielities

honderd euro te doen voor de aankoop van de afsluiterapparatuur. Bovendien moet een aanvuller niet alleen het mobiele telefoonnummer, maar ook de gebruikersnaam en het wachtwoord van een online bankrekening klant achterhalen. Wanneer hij daarmee inlogt, een bedrag overslaat en de transactie bevestigd door een via sms verzonden code of te luisteren, moet hij in bevonden voor zorgen dat hij in de buurt van zijn slachtoffer is. Deze berichten worden alleen verzonden in de nabijheid van de gsm-tower waarmee de mobiele telefoon van het slachtoffer is verbonden. Bovendien moet de mobiele telefoon van het slachtoffer een staat

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

ervraagd trekken steeds tijd en geld uit voor de belang van hun netwerken. aantal beveiliging het aantal

Buiten roken bedreigt IT

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

Algoritme vernietigt zoekprofielen websurfer

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

Gekraakte iPhone is riskant bij bankieren

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

Computer berekent 3D-model van gezichten

De grenscontrole kan een stuk worden vereenvoudigd wanneer de beambte degen die voor hem staat kan verglijken met een 3D-computermodel. Een aantal Amerikaanse staten is inmiddels op een dergelijk systeem overgestapt. De computer toont een ruitje met de combinatie met een foto representatie van het oog. Deze twee plaatjes, die worden gekalke uit een aantal beelden van een video-opname, zijn voldoende voor een snelle identificatie, ondanks dat er zoveel mogelijk is bespaard op berekeningen. Professor Mohamed Abdel-Hafiz van de universiteit van Miami heeft een minimummodel gemaakt, dat alleen rekening houdt met de meest prominente onderdelen van een gezicht. Het gaat dan vooral om de neus, waaierkas, mond en kin. Andere factoren, bijvoorbeeld bolle wangen, spelen een veel minder belangrijke rol voor de herkenning, zo blijkt uit onderzoek. Voor het oog wordt een wat uitgebreide techniek gebruikt, vanwege het grotere aantal variabelen en de verschillende manieren waarop het licht op een neus 'neutraal' kijkt. Er wordt gewerkt aan een systeem dat ook functioneert bij verschillende gezichtsoverdrukkingen.

Tot vijftig procent voorfronteerd met meer dan een halvering van

heid aan dienstverleners in de amse Haven. E-office bouwde nieuw voor Dirkzwager een variant van zijn informatiesysteem te benaderen is via een

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

UMTS-dekking of zee biedt extra veiligheid

cent Oostwade

Indringers verklipt

Hoe herkent u misbruik en welke maatregelen kunt u nemen om te voorkomen dat u wordt misbruikt? Het is belangrijk om de log

Wij investeren ons zelf in firewalls, virusscanners, inbraakdetectiesystemen en peperdure securityconsultants. Dat alles om onze infrastructuur, 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, gfstolen, en laptops kunnen worden misbruikt om via het VPN het bedrijfsnetwerk binnen te dringen. AAD OFFERMAN

'Beveiliging creditcardtransacties onder de maat'

Protocol van Visa en MasterCard afgeleverd
Visa is een single sign-on-systeem, dat geeft de mogelijkheid gebruikers van creditcards bij online bestellingen een wachtwoord te vragen. Webwinklers moeten daarvoor hun systemen aanpassen. Maar de creditcardmaakt stappen maken dat wel aanspreekbaar door het verspreiden van informatie over het gebruik van Visa en MasterCard. Dit heeft de schade aan de beveiliging van creditcardtransacties onder de maat.

De beveiliging van

Wij investeren ons zelf in firewalls, virusscanners, inbraakdetectiesystemen en peperdure securityconsultants. Dat alles om onze infrastructuur, 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, gfstolen, en laptops kunnen worden misbruikt om via het VPN het bedrijfsnetwerk binnen te dringen. AAD OFFERMAN

E-spion heeft hier vrij spel

AIVD brengt procedure uit als waarschuwing tegen digitale spionage

ECM Annelke Houtman

Het Steunpunt Acquisitiefraude waarschuwt voor digitale spookfacturen. De verscherpte Spin-wetgeving verlaagt de drempel voor malitieuze bedrijven om nepnotas te versturen. Platform Elfa (Elktronisch Factureren) raadt bedrijven aan een witte en een zwarte lijst op te stellen van respectievelijk bedrijven waar

Spam-wet verlaagt drempel e-spookfactuur

zaken worden gedaan en verdachte ondernemingen. Een voorbeeld van een digitale spookfactuur is de mail die afkomstig is van de 'Gele Bedrijfsreiger'. Het bedrijf 'verzoekt' ondernemers hun bedrijfsgegevens te controleren en de pdf-bijlage onderkend per fax terug te sturen. Het logo van de Gele Bedrijfsreiger lijkt sterk op dat van de Gouden Gids. Als de ondernemer de fax terugstuurt, tekent hij door een overeenkomst waar hij

Spam-wet verlaagt drempel e-spookfactuur

zaken worden gedaan en verdachte ondernemingen. Een voorbeeld van een digitale spookfactuur is de mail die afkomstig is van de 'Gele Bedrijfsreiger'. Het bedrijf 'verzoekt' ondernemers hun bedrijfsgegevens te controleren en de pdf-bijlage onderkend per fax terug te sturen. Het logo van de Gele Bedrijfsreiger lijkt sterk op dat van de Gouden Gids. Als de ondernemer de fax terugstuurt, tekent hij door een overeenkomst waar hij

THINKSECURE

THINKSECURE

THINKSECURE

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 geraffineerdheid. 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