



Er zitten gaten in de chinese muur.

Zoals bekend past China censuur toe voor haar burgers op het internet. Hiertoe heeft China een grote firewall geplaatst die al het internetverkeer filtert op "verkeerde" woorden. Onlangs heeft Richard Clayton van de universiteit van Cambridge "gaten" ontdekt in de methode die wordt gehanteerd.

Het filteren en vervolgens blokkeren van verkeer en dan ook nog een acceptable throughput te houden is erg complex.

Het blijkt dat het verkeer ook niet wordt gefilterd op routers aan de rand van de chinese netwerken, maar op andere systemen. Deze systemen blokkeren het verkeer niet, maar zenden naar de browser en naar de server TCP reset pakketten, indien in de datastream woorden voorkomen die op de censuurlijst voorkomen. Beide kanten denken dat de andere kant de sessie wil beëindigen en de verbinding wordt verbroken. Op deze manier wordt er gecensureerd.

Als beide kanten echter de TCP reset pakketten negeren, blijft de sessie gewoon bestaan.

Het negeren van TCP reset pakketten is te bereiken met behulp van firewall rules. Ook zou, met wat meer inspanning aan de hand van TTL hop counts kunnen worden nagegaan dat de TCP resets niet van de andere kant zijn, maar van een derde partij.

Het sturen van TCP reset pakketten zijn bekende aanvalstechnieken (Denial of Service attacks). De trend is dat er meer en meer programmatuur (operating systemen, applicaties) op de markt komen die niet gevoelig zijn voor een dergelijke "aanval". In het geval dat deze programmatuur wordt gebruikt, zal deze vorm van censuur in het geheel niet meer werken.

Richard Clayton heeft de resultaten van het onderzoek naar de chinese firewall op 28 juni in een workshop m.b.t. privacy enhancing technologies in Cambridge gepresenteerd.

Natuurlijk worden, naast bovengenoemde techniek ook andere technieken gebruikt om te voorkomen dat chinese burgers over informatie beschikken, waarvan de overheid niet wil dat ze binnen China worden verspreid. Zo worden bepaalde websites gewoon geblokkeerd.

Bovenstaande is een voorbeeld van een lek en toont aan dat het onmogelijk is om in dit tijdperk alle informatiestromen te controleren.

Bron: <http://www.lightbluetouchpaper.org/2006/06/27/ignoring-the-great-firewall-of-china/>

Secure Connection levert Compliance kennisobjecten

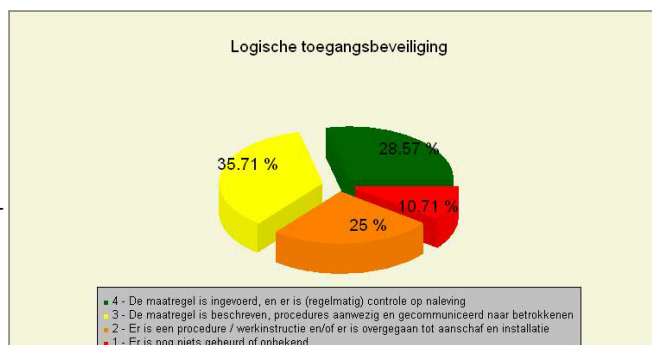
Recent heeft Secure Connection een nieuw programma ontwikkeld: Compliance Builder. Met dit programma kunnen kennisobjecten (Compliance objecten) worden gebouwd.

Met deze compliance builder is het mogelijk om in uw organisatie een self-assessment of een compliance check uit te (laten) voeren, waarbij u zelf bepaald langs welke norm er moet worden gemeten. U kunt uw eigen norm of een externe norm, zoals ISO 17799, Cobit of Sarbanes Oxley vanuit een Word formaat, excel formaat of een ander gangbaar formaat omzetten in een kennisobject. U dient hierbij zelf aan

te geven welke maturity levels u wilt gebruiken, en welke verantwoordelijke functionarissen u aan welke richtlijn wilt koppelen. Ook kunt u de de richtlijnen uit de norm in groepen verdelen.

Het kennisobject kan vervolgens vragenlijsten per functionaris afdrucken.

Het compliance object kent verschillende grafische objecten voor uw (management-) rapportage.



Bovengenoemd programma is één van de programma's van Secure Connection, waarmee het mogelijk is om zelf kennisobjecten te bouwen en te onderhouden.

Vanzelfsprekend kunnen wij ook een maatwerk kennisobject voor u leveren. Gelet op de krachtige programma's die ons ten dienste staan, kunnen wij maatwerkobjecten snel leveren.

U kunt een brochure met meer gegevens over Compliance Builder downloaden via onze website <http://www.seccon.nl> Ook hebben wij een brochure bijgevoegd.

Actueel

Kwaadaardig macro virus

Berichten over virussen en malware, die via emails worden verspreid verschijnen wekelijks. De beste remedie tegen dergelijke aanvallen blijft u zelf. Open nooit attachments van email van onbekenden of "verdachte" email van bekenden. Dit geldt niet alleen voor executables, maar ook voor officebestanden, zoals wordbestanden.

Onlangs is weer een lek ontdekt in MSWord 2002 en ouder.

Een kwaadaardige wordmacro wordt verpakt in een document, genaamd "my_Notebook.doc". Dit bestand bevat het Kukudro virus. Dit macrovirus (geschreven in VBA) decodeert een binary file en plaatst deze als 666inse_1.exe en start deze vervolgens op. Deze executable is een trojan downloader, genaamd Small.dcu. Het resultaat is dat u een heleboel malware op uw PC krijgt.

Bron: http://www.f-secure.com/v-descs/kukudro_a.shtml