Stichting NIOC en de NIOC kennisbank

Stichting NIOC (www.nioc.nl) stelt zich conform zijn statuten tot doel: het realiseren van congressen over informatica onderwijs en voorts al hetgeen met een en ander rechtstreeks of zijdelings verband houdt of daartoe bevorderlijk kan zijn, alles in de ruimste zin des woords.

De stichting NIOC neemt de archivering van de resultaten van de congressen voor zijn rekening. De website www.nioc.nl ontsluit onder "Eerdere congressen" de gearchiveerde websites van eerdere congressen. De vele afzonderlijke congresbijdragen zijn opgenomen in een kennisbank die via dezelfde website onder "NIOC kennisbank" ontsloten wordt.

Op dit moment bevat de NIOC kennisbank alle bijdragen, incl. die van het laatste congres (NIOC2023, gehouden op donderdag 30 maart 2023 jl. en georganiseerd door NHL Stenden Hogeschool). Bij elkaar bijna 1500 bijdragen!

We roepen je op, na het lezen van het document dat door jou is gedownload, de auteur(s) feedback te geven. Dit kan door je te registreren als gebruiker van de NIOC kennisbank. Na registratie krijg je bericht hoe in te loggen op de NIOC kennisbank.

Het eerstvolgende NIOC vindt plaats op donderdag 27 maart 2025 in Zwolle en wordt dan georganiseerd door Hogeschool Windesheim. Kijk op www.nioc2025.nl voor meer informatie.

Wil je op de hoogte blijven van de ontwikkeling rond Stichting NIOC en de NIOC kennisbank, schrijf je dan in op de nieuwsbrief via

www.nioc.nl/nioc-kennisbank/aanmelden nieuwsbrief

Reacties over de NIOC kennisbank en de inhoud daarvan kun je richten aan de beheerder:

R. Smedinga kennisbank@nioc.nl.

Vermeld bij reacties jouw naam en telefoonnummer voor nader contact.

Wat kunnen we leren van Wikileaks

Auteurs
Dr. Bert Melief
M&I/Partners en HS Zuyd
Email: bert.melief@mxi.nl

Ir. Willem Kossen
M&I/Partners
Email: willem.kossen@mxi.nl

Samenvatting
Dit artikel gaat over bewustwording. De publicaties door Wikileaks die de afgelopen tijd in het nieuws waren dienen als voorbeeld voor het gebrek aan actueel inzicht in de beveiliging van vertrouwelijke gegevens, tot op de hoogste politieke en bestuurlijke niveaus. Naast enige technische overwegingen geven we tips hoe iedereen, maar vooral ook mensen die werkzaam zijn in het onderwijs, met deze materie om zou kunnen gaan.

Wat kunnen we leren van Wikileaks

De eerste vraag is: Hoeveel mensen hadden toegang tot de diplomatieke USA bronnen voordat Wikileaks die heeft ontsloten? Niemand kwam ook maar in de buurt van het goede antwoord: ca. 3 miljoen mensen! Dat heeft de Engelse krant 'the Guardian' tamelijk overtuigend aangetoond.
Daarmee geven we een van de belangrijkste redenen aan voor alle commotie rond de veiligheid van het Internet. Wij gaan ontzettend slordig om met onze soms zeer vertrouwelijke gegevens.

Volgende vraag is: heb je wel eens een mail met PKI verstuurd? Hoe vaak check je of je bij het internetbankieren wel een beveiligde website gebruikt? Hoe kan het dat we nog steeds bestookt worden met Phishing mails (bv. vragen naar toegangsgegevens onder een dekmantel)? Je kunt met https naar facebook, doe je het ook?
De antwoorden spreken boekdelen. Prive gebruik van PKI komt vrijwel nooit voor. En ook de andere vragen leverden tamelijk duidelijke antwoorden op: we zijn ons er nauwelijks van bewust dat we zorgvuldig moeten omgaan met onze gegevens.

1 Wat betekent dit allemaal?

Is Assange een boef die achter de tralies moet? Moeten we internetverkeer gaan beperken? Is aanvullende wetgeving nodig? En doe je dat Nationaal/ Europees?

Alles wat je op Internet publiceert is in principe onvergankelijk en publiek: 'The Internet Archive'. En dat is een groot contrast met vroeger: in de tweede wereldoorlog kon je de joden redden door het lokale archief (met etnische registratie-gegevens) in brand te steken. In de digitale wereld is informatie niet vergankelijk en zodanig gedistribueerd dat vernietiging vrijwel onmogelijk is geworden!
Bovendien, van wie zijn 'jouw' gegevens eigenlijk?

We geven vier tips voor de komende generatie:

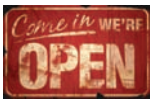
1 Hoe te voorkomen dat we telkens de put willen dempen als het kalf al verdronken is?
Wikileaks is daar een fraai voorbeeld van. Hoe kun je dat voor zijn: naar ons inzicht door een combinatie van gezond verstand en het houden van toezicht. Zorg dat je situaties voor bent waarin het kwaad al is geschied. Want voorkomen is beter (goedkoper) dan genezen.

2 Verhelder de onderliggende structuren.
Als je weet hoe iets in elkaar zit, kun je het beter beheersen. Hier zit een uitdaging voor het ICT onderwijs. Als mensen zich bewust zijn van de intrinsieke openheid van Internet en als ze weten dat niet iedere gebruiker van goeie wil is kan je zorgen dat je van lapmiddel naar preventieve maatregel komt.

3 Beperken van verkeer is niet de oplossing

De bits en bytes zijn onschuldig. De protocollen (TCP/IP) zijn onschuldig. Het gaat om content en de gebruikers ervan (gedrag). De schade van aantasting van de 'vrijheid van verkeer' is vele malen groter dan de te behalen baten met het beperken ervan. De economie van de 21ste eeuw is niet meer denkbaar zonder vrij Internet verkeer. Bovendien: als een bankrover over de snelweg rijdt, schaf je de snelweg toch niet af.

4 Het beveiligen van Assets is nodig, maar dat doen we nog niet.



Wie mag wanneer onder welke voorwaarden waarvan gebruik maken? Daarvoor zijn technische hulpmiddelen beschikbaar: Role Based Access Control (RBAC) en Identity and Access Management (IAM). Daarnaast kan iedere gebruiker (bedrijf/organisatie, maar ook privé persoon) met een beetje moeite zorgen voor bewust classificeren van informatie op basis van inhoudelijke argumentatie. De rest kan je open laten (Open Tenzij).

2 Wat kan het onderwijs doen?

Heel belangrijk is het bijbrengen van bewustwording bij leerlingen over de onderliggende problematiek (geef kijkjes onder de motorkap). Daar zijn prachtige voorbeelden van. Wikileaks is natuurlijk al een heel mooie praktijk case. Een tweede (die zich voordeed na NIOC 2011) is de nationale consternatie die ontstond door het drama rond Diginotar, waarbij een leverancier van beveiligingscertificaten zelf onprofessioneel opereerde.

Een van de belangrijkste elementen is natuurlijk gedragsbeïnvloeding: het is van belang dat leerlingen doorkrijgen dat niet alle 'veilige' sites echt veilig zijn. Van zogenaamde Phishing detectie tot gewoon bewustzijn (check of je het 'slotje' ziet)
En: goed voorbeeld doet goed volgen. De bronnen van de school zijn adequaat beveiligd.