**Potentiële onderwijs projecten CyberDEW**

|  |  |
| --- | --- |
| **Case 1** | **Indexeren van het risico profiel van nieuwe werknemers** |
| Opleiding | CMD / MT |
| Onderwerp | Aan de hand van leeftijd, geslacht, opleiding, anti-phishing training, methode van training, internet gebruik, persoonlijkheid en gedrag kunnen er uitspraken worden gedaan over de kans dat een werknemer valt voor een phishing mail. Dat wil zeggen dat hij de mail opent, doorklikt en er daardoor een serieuze malware dreiging ontstaat, waarbij er bijvoorbeeld bedrijfsgegevens kunnen worden gestolen.  Om het risico profiel van werknemers te indexeren moeten bovenstaande gegevens worden geïnventariseerd. Sommige gegevens zoals leeftijd, geslacht, opleiding, anti-phishing training, methode van training zullen bij een werkgever aanwezig zijn. Om het profiel compleet te maken zijn echter ook de gegevens over werknemers hun internet gebruik, persoonlijkheid en gedrag essentieel. Dit zal een grootschalige inventarisatie actie vereisen. Daarnaast zal er om de gegevens up to date te houden ook van elke nieuw aangestelde medewerker een risico profiel moeten worden opgesteld.  Ontwerp een tool waarmee de risico profielen van nieuwe en oude werknemers in kaart kunnen worden gebracht. Denk daarbij aan de volgende vragen:  Wat moet een risico profiel precies bevatten? Wat voor gegevens zijn er nodig om werknemers hun internet gebruik, persoonlijkheid en gedrag in kaart te brengen? Hoe kan een risico profiel zo gebruiksvriendelijk, efficiënt en accuraat mogelijk worden opgesteld? |
| Literatuur | A. Darwish, A. El Zarka, and F. Aloul, “Towards Understanding Phishing Victims ’ Profile,” pp. 13–17, 2013. |
| Contactpersoon | CMD - Peter van Waart (p.van.waart@hr.nl) & MT – Emiel Bakker (e.p.bakker@hr.nl) |

|  |  |
| --- | --- |
| **Case 2** | **Het waarderen en integreren van weak security alerts in het cyber security systeem** |
| Opleiding | INF |
| Onderwerp | Aan de hand van leeftijd, geslacht, opleiding, anti-phishing training, methode van training, internet gebruik, persoonlijkheid en gedrag kunnen er uitspraken worden gedaan over de kans dat een werknemer valt voor een phishing mail. Dat wil zeggen dat hij de mail opent, doorklikt en er daardoor een serieuze malware dreiging ontstaat, waarbij er bijvoorbeeld bedrijfsgegevens kunnen worden gestolen.  In het CyberDEW defense shield wordt menselijke kennis gebruikt om het systeem technisch te verbeteren (machine learning). Het is daarbij echter essentieel dat het systeem leert van accurate informatie, daarom wordt er aan het report van de werknemers een waarde toegevoegd op basis van hun risico profiel. Deze waarde dient als een indicator die iets zegt over de betrouwbaarheid van de door de werknemer opgestelde (weak) alert. Op basis van deze waarde zal het systeem de informatie wel of niet gebruiken om zijn ‘rules’ aan te scherpen.  Bouw een systeem dat zichzelf verbeterd op basis van de door de werknemers gegenereerde weak alerts. Ga na welke informatie een alert report moet bevatten om het systeem te laten leren. Bedenk daarbij hoe je om gaat met de waarde die er aan de betrouwbaarheid van een profiel en daarmee een alert gegeven is. |
| Literatuur | A. Darwish, A. El Zarka, and F. Aloul, “Towards Understanding Phishing Victims ’ Profile,” pp. 13–17, 2013. |
| Contactpersoon | INF - Kevin van Ingen (ingkl@hr.nl) |

|  |  |
| --- | --- |
| **Case 3** | **In kaart brengen en gebruikmaken van mailgedrag van werknemers en patronen in inkomende bedrijfsmail** |
| Opleiding | INF |
| Onderwerp | In een grote organisatie wordt er per dag frequent heen en weer gemaild tussen werknemers. Naast intern mailverkeer komt er ook mail van buiten de organisatie binnen. In verband met de preventie van bedrijfsspionage door spear-phishing aanvallen is het mogelijk interessant om deze netwerken in kaart te brengen en de frequentie en inhoud van de emails (tone of voice) te gebruiken om verdachte mails te identificeren.  Onderzoek of er vaste patronen in het mailverkeer van werknemers in bedrijfscontext te herkennen zijn. Met welke collega’s mailen werknemers frequent? Mailen de werknemers ook met hun baas of de directeur van een organisatie en beïnvloed dit de ‘tone of voice’ van de email? Wat voor invloed heeft een bulk mail vanuit een facilitair deel van de organisatie? Kan het interne netwerk in verband worden gebracht of worden vergeleken met bijvoorbeeld de oorsprong en frequentie van inkomende mails van buitenaf? |
| Literatuur | Aycock J. (2007) A design for an anti-spear-phishing system. Department of Computer Science, University of Calgary, Calgary, Alberta, Canada. |
| Contactpersoon | INF - Kevin van Ingen (ingkl@hr.nl) |

|  |  |
| --- | --- |
| **Case 4** | **Kosten en baten van cyber security systemen binnen een bedrijfscontext** |
| Opleiding | CMD / CDM / COM |
| Onderwerp | Om bedrijfsgegevens veilig te stellen voor diefstal worden er per jaar miljarden euro’s uitgegeven aan cyber security systemen. Menselijk gedrag heeft echter veel invloed op het functioneren van deze systemen. Daarom wordt er getracht om security policies voor te schrijven en te handhaven om zo te zorgen dat werknemers zich aanpassen aan deze systemen. Het wordt echter steeds duidelijker dat deze methoden niet werken, omdat de systemen en security policy niet afgestemd zijn op de menselijke maat. Het naleven van de opgestelde regels kost werknemers doorgaans veel handelingen en tijd, dit leidt vaak tot irritatie. Hierdoor worden de regels vaak niet nageleefd, met ernstige malware bedreigingen als gevolg.  Doe daarom onderzoek naar het handhaven van security policies binnen een bedrijfscontext. Stel daarbij vragen als: kunnen cyber security systemen worden aangepast aan de menselijke maat? Kan er hierbij gebruik worden gemaakt van HCI methoden? Wat zijn incentives om werknemers mee te laten werken met de security policy binnen de bedrijfscontext? Hoe kunnen systemen beter worden afgestemd op menselijk gedrag en andersom? Kan er daarbij beter worden omgegaan met aspecten als tijdsinvestering en werkonderbreking? |
| Literatuur | Beautement A, Sasse A.M, Wonham M. (2008) The Compliance Budget: Managing Security Behaviour in Organisations. NSPW’08, Lake Tahoe, California, USA. |
| Contactpersoon | CMD - Peter van Waart (p.van.waart@hr.nl) & CDM - Stan Scheerder (c.j.t.m.scheerder@hr.nl) & COM – Komala Mazerant-Dubois (k.mazerant-dubois@hr.nl) |

|  |  |
| --- | --- |
| **Case 5** | **Adequate en frequente feedback en inzicht in bedreigingen voor alle lagen van een bedrijf** |
| Opleiding | CMD / MT / INF |
| Onderwerp | Om bedrijfsgegevens veilig te stellen voor diefstal worden er per jaar miljarden euro’s uitgegeven aan cyber security systemen. Menselijk gedrag heeft echter veel invloed op het functioneren van deze systemen. Daarom wordt er getracht om security policies voor te schrijven en te handhaven om zo te zorgen dat werknemers zich aanpassen aan deze systemen. Het wordt echter steeds duidelijker dat deze methoden niet werken, omdat de systemen en security policy niet afgestemd zijn op de menselijke maat. Het naleven van de opgestelde regels kost werknemers doorgaans veel handelingen en tijd, dit leidt vaak tot irritatie. Hierdoor worden de regels vaak niet nageleefd, met ernstige malware bedreigingen als gevolg.  Onderzoek of real-time feedback over security dreigingen een rol speelt in de communicatie naar medewerkers binnen grote organisaties. Zijn medewerkers meer geneigd om zich te houden aan de security policies? Kunnen malware dreigingen in kaart worden gebracht en worden gevisualiseerd? Moeten deze visualisaties worden teruggekoppeld naar de werknemers? Zo ja, hoe moet deze terugkoppeling plaatsvinden, denk aan frequentie, timing, boodschap, educatie, medium, etc. |
| Literatuur | P. Dourish and D. Redmiles () Approach to Usable Security Based on Event Monitoring and Visualization. Information and Computer Science, University of California, Irvine, CA 92697-3425, USA.  A. Komlodi, P. Rheingans, U. Ayachit, J.R. Goodall and A. Joshi (2005) A User-centered Look at Glyph-based Security Visualization. Workshop on Visualization for Computer Security October 26, Minneapolis, MN, USA, IEEE.  A. Komlodi, J.R. Goodall and W.G. Lutters (2004) An Information Visualization Framework for Intrusion Detection. Department of Information Systems, UMBC  1000 Hilltop Circle, Baltimore, MD 21250, USA. CHI 2004. |
| Contactpersoon | CMD - Peter van Waart (p.van.waart@hr.nl) & MT – Emiel Bakker (e.p.bakker@hr.nl) & INF - Kevin van Ingen (ingkl@hr.nl) |

|  |  |
| --- | --- |
| **Case 6** | **Security awareness en betrokkenheid op de werkvloer** |
| Opleiding | CDM / COM |
| Onderwerp | Een (spear-)phishing vindt doorgaans plaats via een externe aanval. Het komt echter ook voor dat phishers van binnen een bedrijf aanvallen, een zogenaamde interne aanval.  Een interne (spear-)phishing aanval kan op verschillende manieren plaatsvinden: (1) Een kwaadwillende werknemer, in dit geval de phisher, kan zijn werkgevende organisatie van binnenuit aanvallen. (2) Een phisher kan letterlijk een bedrijf binnenlopen en zijn computer in het netwerk van de desbetreffende organisatie pluggen. Waarschijnlijker is echter dat de phisher met zijn eigen computer inlogt op een onbeveiligd wireless netwerk van een organisatie en zo de firewall van een bedrijf omzeilt. (3) De phisher kan echter ook een phishing mail sturen vanaf de computers van het betreffende bedrijf zelf. Hij kan dit opnieuw doen door letterlijk het bedrijf binnen te lopen, te kijken of hij een password slingert bijvoorbeeld geschreven op een post-it geplakt onder een toetsenbord, zodat hij hiermee in de computer kan inloggen om zijn (spear-)phishing email te verzenden.  Deze methode brengt echter veelrisico met zich mee, een andere methode om de email van één van de organisaties computers te versturen is door een USB stick te laten slingeren in bijvoorbeeld de parkeergarage van een bedrijf. Als een werknemer de USB stick vind en inplugt, zal er malware worden geïnstalleerd en de (spear-)phishing email van binnenuit de organisatie worden verstuurd.  Dit fenomeen is lastig te ondervangen door middel van cyber security technologie. Preventie hangt voornamelijk af van de oplettendheid van werknemers. Communicatie strategieën om werknemers bewust te maken van dit fenomeen zijn hiervoor evident. Wat voor communicatie kanalen moeten er worden gebruikt om werknemers voor te lichten? Wat kunnen werknemers doen om een steentje bij te dragen aan preventieve maatregelen? Hoe en waar kunnen verdachte activiteiten worden gemeld? Wat wordt er met die informatie gedaan en wat voor feedback wordt er gegeven aan actieve medewerkers? |
| Literatuur | Paul Dourish Æ Rebecca E. Grinter Jessica Delgado de la Flor Æ Melissa Joseph Security in the wild: user strategies for managing security as an everyday, practical problem. |
| Contactpersoon | CDM - Stan Scheerder (c.j.t.m.scheerder@hr.nl) & COM – Komala Mazerant-Dubois (k.mazerant-dubois@hr.nl) |

|  |  |
| --- | --- |
| **Case 7** | **Omgaan met power bias tussen deelnemers en de huidige invloed of mogelijke toekomstige invloed van phishers op de creatie van weak alerts door eindgebruikers** |
| Opleiding | INF? |
| Onderwerp | PhishTank is een website waarop mensen phishing aanvallen kunnen melden. Deze vorm van crowdsourcing biedt het perspectief om phishing aanvallen eerder te detecteren en zo succesvolle phishing aanvallen te voorkomen.  Er is echter geconcludeerd dat voornamelijk dezelfde deelnemers op dit platform participeren. Hierdoor wordt er niet optimaal gebruik gemaakt van de ‘Wisdom of the Crowd’ en worden de conclusies op basis van deze meldingen minder accuraat. Verder is er een vergroot risico dat de phisher zelf in het netwerk van deelnemers infiltreert en zo het systeem negatief beïnvloed.  Ga na wat de huidige invloed is van één enkele deelnemer op het systeem. Hoe kan de invloed van één enkele deelnemer worden verminderd of worden gespreid? Hoe kan er worden voorkomen dat de phisher(s) zelf mee gaan participeren in het systeem? Hoe kan er worden gezorgd dat deelnemers die minder frequent participeren, frequenter alerts gaan toevoegen? Hoe kan de kwaliteit en de betrouwbaarheid van de meldingen worden vergroot? |
| Literatuur | T. Moore and R. Clayton, “Evaluating the Wisdom of Crowds in Assessing Phishing Websites,” pp. 1–15, 2007. |
| Contactpersoon | INF - Kevin van Ingen (ingkl@hr.nl) |

|  |  |
| --- | --- |
| **Case 8** | **Phishing markt en productonderzoek** |
| Opleiding | INF / MT / CDM? |
| Onderwerp | Er zijn diverse producten bedacht om (spear-)phishing tegen te gaan. Een aantal van deze producten kunnen gratis online worden gebruikt. Deze producten zijn echter vaak onbekend bij het grote publiek. Naast gratis producten worden er commerciële producten veelal door kleine bedrijven aangeboden. Zij proberen hun producten te verkopen aan grotere organisaties in diverse sectoren. Weer een andere categorie producten wordt ontwikkeld voor wetenschappelijke doeleinden. Deze producten zijn doorgaans niet in gebruik door het grote publiek, maar dienen als onderzoeksmateriaal voor het publiceren van artikelen.  Om nieuwe producten te ontwikkelen is het belangrijk om huidige oplossingen in kaart te brengen. Breng daarom de huidige (spear-)phishing markt en productoplossingen in kaart. Het is daarbij belangrijk om antwoorden te krijgen op vragen als: welke oplossingen bestaan er om (spear-)phishing tegen te gaan? Wie zijn de afnemers en gebruikers van deze oplossingen? Hoe werken deze oplossingen, zijn die technology-centered producten of user-centered producten? En wat zijn de voor en nadelen van deze oplossingen? |
| Literatuur | Cranor L, Egelman S, Hong J, Zhang Y. (2006) Phinding Phish: An Evaluation of Anti-Phishing Toolbars. CyLab, Carnegie Mellon University, Pittsburgh, PA 15213.  Aycock J. (2007) A design for an anti-spear-phishing system. Department of Computer Science, University of Calgary, Calgary, Alberta, Canada.  Dong Z, Camp L.J. (2012) Peersec: Towards peer production and crowdsourcing for enhanced security. In The 7th USENIX Workshop on Hot Topics in Security (HotSec). |
| Contactpersoon | INF - Kevin van Ingen (ingkl@hr.nl) & Emiel Bakker (e.p.bakker@hr.nl) & CDM - Stan Scheerder (c.j.t.m.scheerder@hr.nl) |