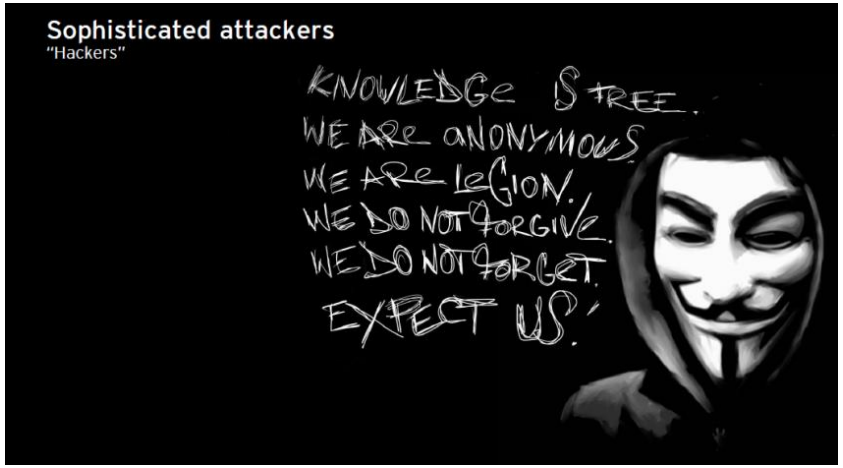
Cybersecurity

Ledenbijeenkomst Brainport Industries - 12 oktober 2017

Sandra Konings, Partner BDO Advisory

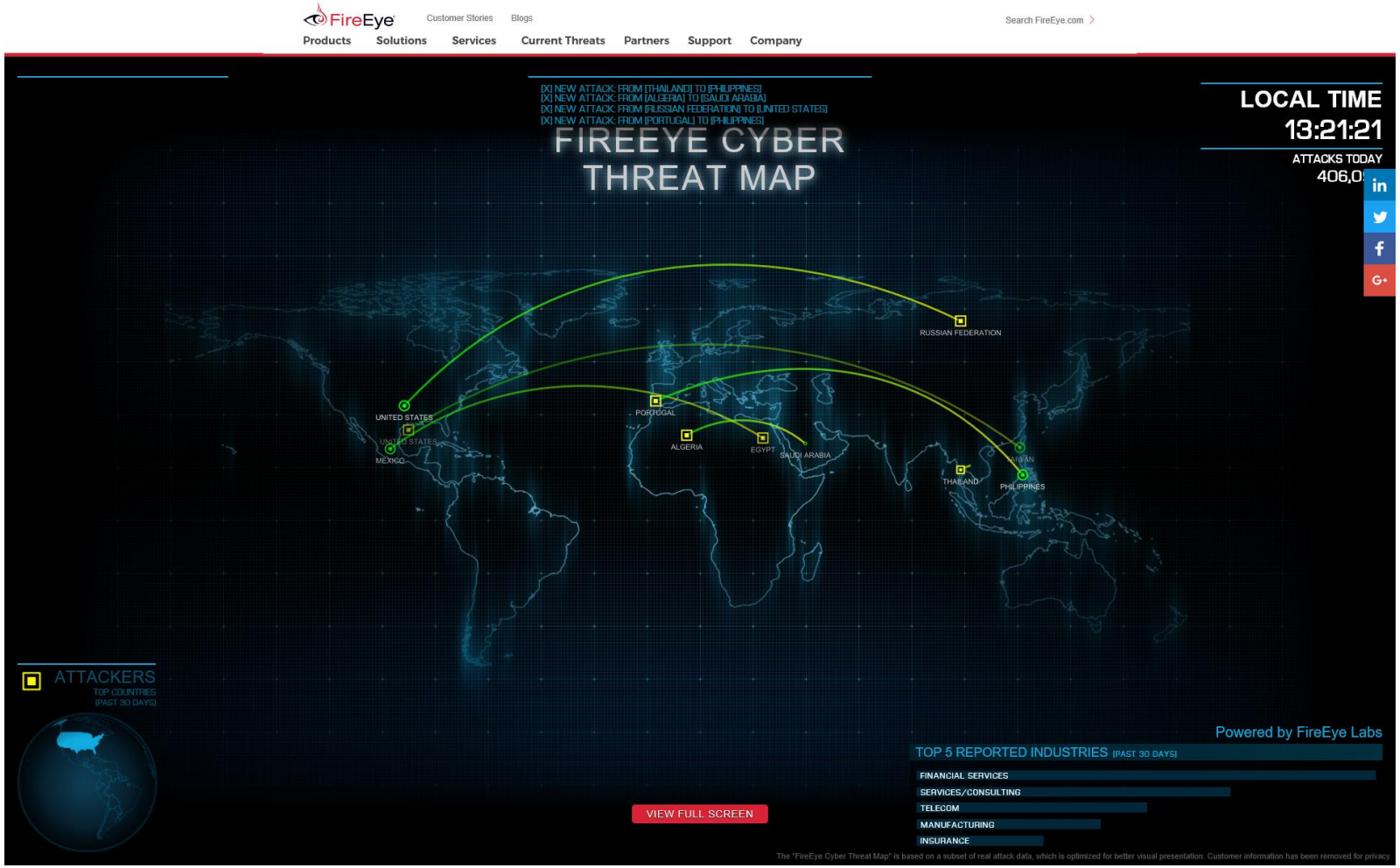
(tevens mede-oprichter en voorzitter Eindhoven Cyber Security Group)

4 vormen van cybercrime



Live cyber attack wereldkaart

(https://www.fireeye.com/cyber-map/threat-map.html)



www.nomoreransom.org

Mag ik uw wachtwoord?

https://youtu.be/opRMrEfAIil?t=42

Wat doet onze overheid?

CSR
Cyber Security Council
Cyber Security Raad

POLITIE
High Tech Crime

Nationaal Cyber Security Centrum
Ministerie van Veiligheid en Justitie

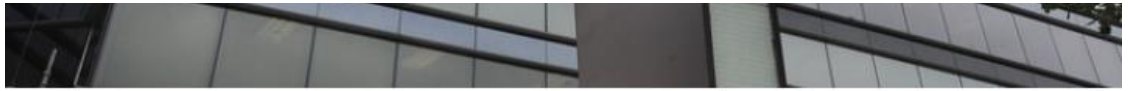
BDO

Mogelijke consequenties

Scholier maakt excuses voor ddos-aanval op betaal-app Bunq

vrijdag 15 september 2017, 14:31 door **Redactie**, 12 **reacties**

De ddos-aanval op de Nederlandse betaal-app Bunq van **vorige week** was het werk van een 18-jarige scholier, die inmiddels tegenover het bedrijf zijn excuses heeft gemaakt, zo laat Bunq zelf weten. Door de aanval was de website van de betaal-app enige tijd slecht of niet bereikbaar en werkte de app traag.



This July 21, 2012, photo shows Equifax Inc., offices in Atlanta. Credit monitoring company Equifax says a breach exposed social security numbers and other data from about 143 million Americans. The Atlanta-based company said Thursday, Sept. 7, 2017, that "criminals" exploited a U.S. website application to access files between mid-May and July of this year. (AP Photo/Mike Stewart) © AP

Hackers stelen persoonsgegevens van miljoenen Amerikanen

Het kredietbureau Equifax is getroffen door een cyberaanval. Hackers hebben daardoor toegang gekregen tot creditcardgegevens, huisadressen, geboortedata en andere persoonlijke informatie van mogelijk 143 miljoen Amerikanen.

© ANP

Wereldwijde hack legt bedrijven en Rotterdamse terminal plat

UPDATE | Voor de tweede keer in korte tijd hebben computercriminelen tientallen bedrijven lamgelegd met een wereldwijde ransomware-aanval. In Nederland liggen twee grote containerterminals in de Rotterdamse haven sinds gistermiddag stil. Ook farmaceut MSD, pakketbezorger TNT en de 38 vestigingen van bouwmaterialenleverancier Raab Kärcher zijn getroffen.

Mogelijke consequenties

- **Reputatieschade en/of financiële schade**

  Klanten, businesspartners of de concurrent kunnen vraagtekens plaatsen bij de veiligheid van uw systemen of werkwijze wanneer een hack wereldkundig wordt gemaakt. Reputatieschade is meestal de reden waarom bedrijven een aanval stilhouden.

- **Politieke reputatieschade**

  In sommige gevallen verkondigen cybercriminelen ideologische of politieke boodschappen via de gehackte website of social-mediakanalen van een bepaalde organisatie. Vaak zijn dit boodschappen die haaks staan op de boodschap van deze organisatie en de opvattingen van haar doelgroep. Deze vorm van cybercriminaliteit komt niet veel voor in Nederland.

- **Verminderde bereikbaarheid**

  Een DDoS-aanval levert meestal geen permanente schade op maar zorgt ervoor dat een website enige tijd niet bereikbaar is. In het geval van een grote webshop of een SaaS-oplossing richt een tijdelijk slechte bereikbaarheid directe financiële schade aan. Wanneer de aanval in het nieuws wordt besproken is reputatieschade een tweede gevolg van verminderde bereikbaarheid.

- **Niet voldoen aan wet- en regelgeving**

  Als persoonsgegevens op straat komen te liggen naar aanleiding van een hack, is een organisatie verplicht dit te melden bij de Autoriteit Persoonsgegevens. Als blijkt dat de beveiliging van deze data niet op orde was, kunnen forse boetes worden opgelegd.

8 tips voor preventie en detectie van cybercrime

Tip 1: Blijf bij met ICT security updates en standaarden

Tip 2: Zorg voor tijdige detectie en ken uw kwetsbaarheden

Tip 3: Bescherm uw kroonjuwelen

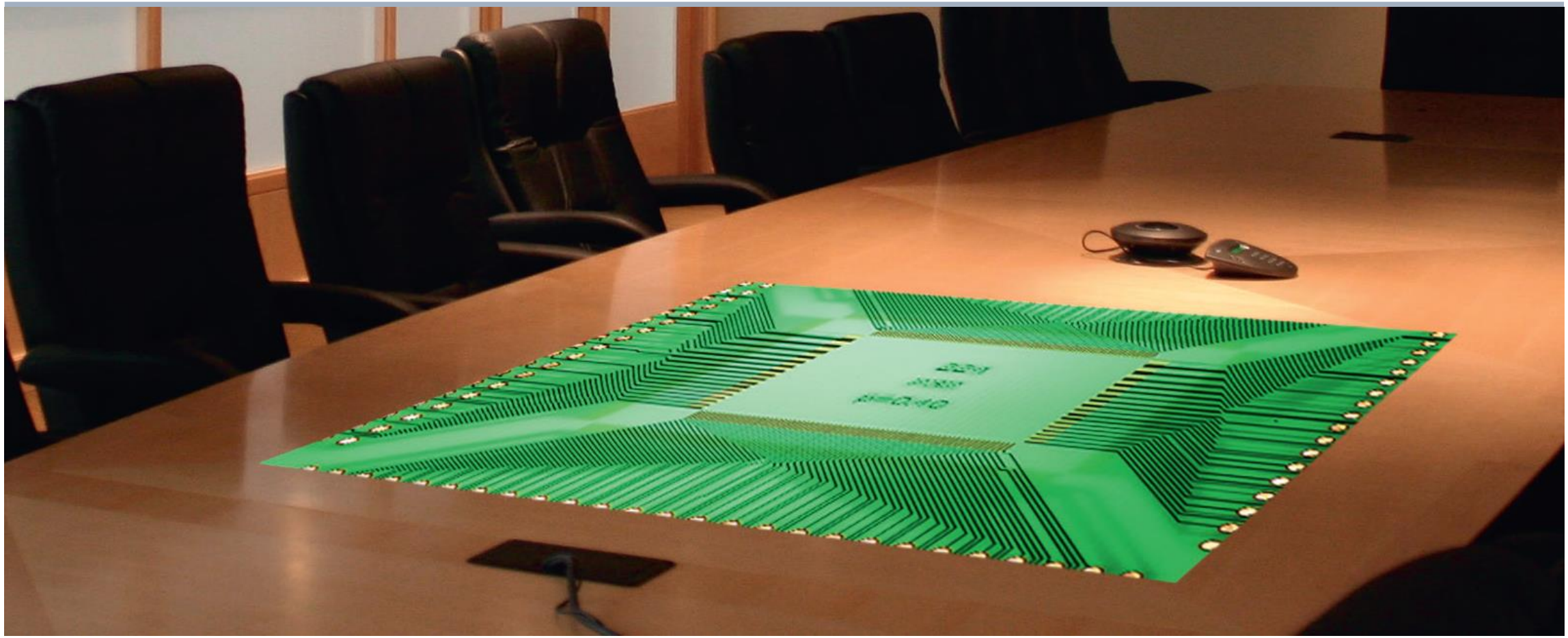
Tip 4: Houd uw internal control op orde

Tip 5: Stel security eisen aan uw leveranciers en afnemers

Tip 6: Werk samen in uw strijd tegen cybercrime

Tip 7: Maak uw medewerkers bewust van cybergevaren

Tip 8: Bespreek cyber risico's in de Boardroom



8 tips voor preventie en detectie van cybercrime

Voor meer informatie en advies

Consultancy cybersecurity & privacy

Ir. S.J.C. (Sandra) Konings

Sandra.Konings@bdo.nl

Partner BDO Advisory

Voorzitter Eindhoven Cyber Security Group

Tel. +31 30 284 9960

Mob. +31 6 5150 8151

Ronde Tafel Discussie – 5 thema's

1. Cybersecurity in de keten
2. Cybersecurity in de industriële omgeving
3. Cybersecurity bewustwording
4. Cybersecurity op orde?
5. Cyberweerbaarheid MKB

Cybersecurity

BDO Advisory B.V.

Van Deventerlaan 101, 3528 AG Utrecht

Postbus 4053, 3502 HB Utrecht

www.bdo.nl/cybersecurity