Basic principles of cyber security

17/05/2018

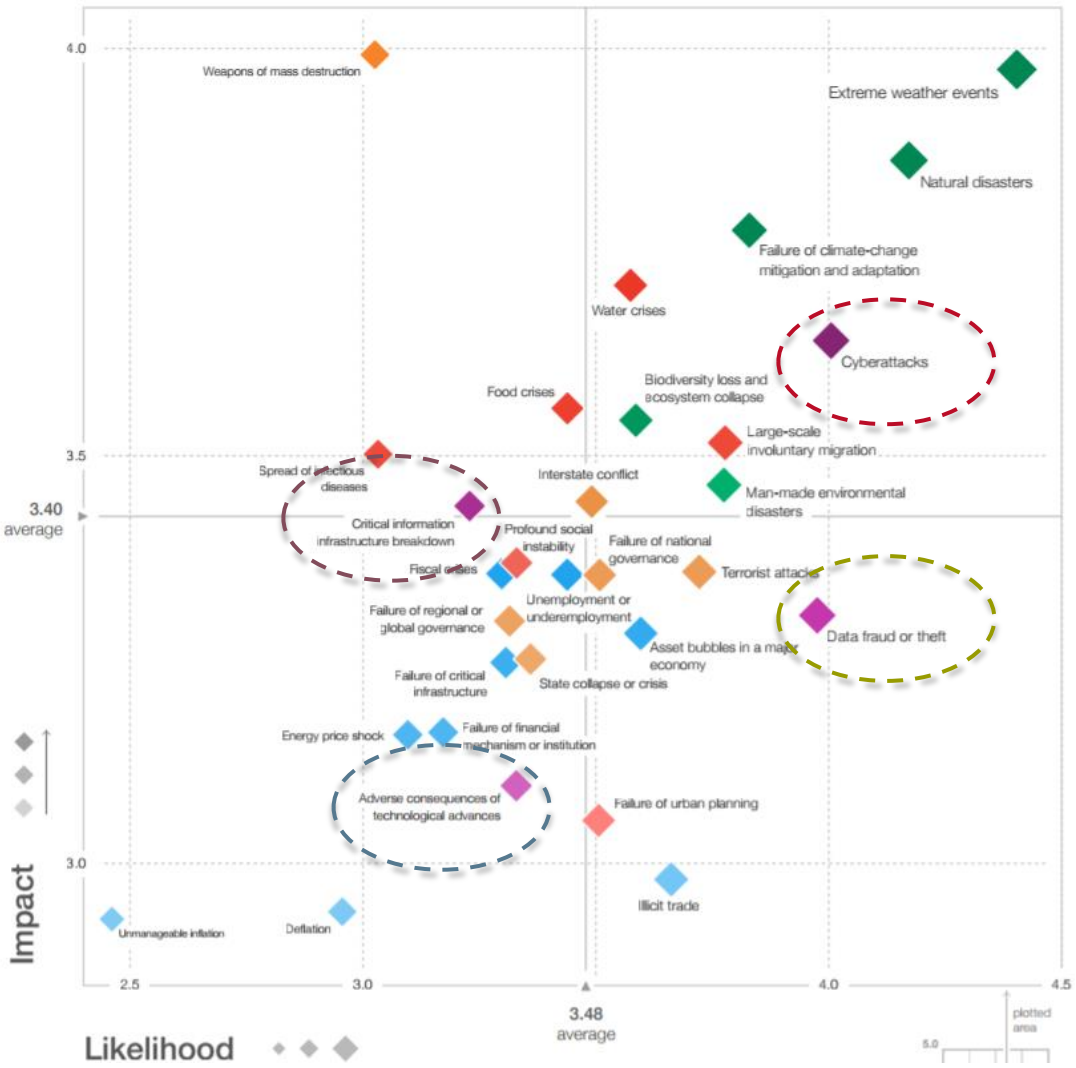
It’s not an IT thing only

Port of Antwerp

European Tugowners Association - Antwerp

Setting the scene

WEF Global Risks report – editie 2018



- **Cyber attacks**
- **Data theft / fraud**
  (> GDPR impact !)
- **Adverse consequences of tech advances**
- **Critical information infrastructure breakdown**

Responsible versus Accountable

In summary

Join cyber security information sharing networks

Work on resilience

Work on end-user awareness and behaviour

Get the technical foundations right

1

Step 1:

Get the technical foundation right

Key elements to focus on

Key elements to focus on

"The Hygiene factor"

1. Supported operating system
2. Active and enforced patch management
3. Antivirus up to date and enforced
4. Minimal software footprint
5. No administration rights
6. Updated browser version
7. Active and enforced password policy

Idea: Turn this into a KPI

Special focus for PLC- SCADA systems

Nationaal Cyber Security Centrum
Ministerie van Veiligheid en Justitie

Checklist beveiliging van ICS/SCADA-systemen

Factsheet FS-2012-02
versie 1.2 | 22 december 2015

Tref organisatorische én technische maatregelen

Kwaadwillenden en securityonderzoekers tonen interesse in de (on)veiligheid van industriële controlesystemen (ICS/SCADA-systemen). Systemen die direct vanaf het internet bereikbaar zijn liggen in het bijzonder onder vuur. ICS/SCADA-systemen kennen echter meer aandachtspunten. Met behulp van deze factsheet kunt u bepalen of uw ICS/SCADA-systemen afdoende zijn beveiligd. Deze maatregelen worden als good practice beschouwd.

Achtergrond
Het toepassingsgebied van ICS/SCADA-systemen is breed en varieert van eenvoudige tot kritieke systemen en processen. Het is aan de eigenaren om te bepalen welk beveiligingsniveau en diepgang van maatregelen passend zijn. Voor deze bepaling is risicoanalyse noodzakelijk.

Uitgangspunten
In de checklist worden organisatorische en technische maatregelen onderscheiden. Elke maatregel wordt kort toegelicht inclusief referenties naar meer achtergrondinformatie en implementatietips. De checklist omvat maatregelen tegen de meest voorkomende kwetsbaarheden en beveiligingsproblemen.

Doelgroep
Eigenaren en beheerders van ICS/SCADA-systemen en gebouwbeheersystemen.

Samenwerking
Deze factsheet is tot stand gekomen in samenwerking met vertegenwoordigers van de vitale infrastructuur en andere NCSC-partners.

Checklist organisatorische maatregelen

1. De organizatie beschikt over een securitybeleid dat ook van toepassing is op de ICS/SCADA-systemen.
   Veel organizaties hebben wel een securitybeleid, maar ICS/SCADA-systemen vallen niet altijd binnen de reikwijdte van dit beleid. U kunt kiezen voor één beleid voor alle systemen waarbij rekening wordt gehouden met de verschillen tussen de kantoor- en procesomgeving. U kunt ook kiezen voor twee aparte documenten. Een goed beleid draagt bij aan het treffen van de juiste beveiligingsmaatregelen tegen reële risico's.
   Referenties: ISO-27001 [1], hoofdstuk 2.1 van [2], hoofdstuk 4 van [22], hoofdstuk 4.2 van [5], ISA99/IEC62443 [23], hoofdstuk 2 van [24].

2. Het senior management heeft zijn commitment uitgesproken m.b.t. de beveiliging van ICS/SCADA-systemen en handelt hier ook naar.
   Cybersecurity is een gedeelde verantwoordelijkheid van alle medewerkers binnen een organizatie en in het bijzonder van leidinggevenden. Zorg voor heldere afspraken met het senior management over het belang van de beveiliging van ICS/SCADA-systemen, de inzet van de benodigde resources en het budget om maatregelen te treffen waar nodig.
   Referenties: hoofdstuk 4.2 van [5], hoofdstuk 1 van [24].

3. Risicomanagement wordt toegepast op alle bedrijfsprocessen, inclusief de voor de primaire processen verantwoordelijke ICS/SCADA-systemen. Incidentmanagement, inclusief managementrapportage, is ook ingericht voor de ICS/SCADA-systemen.
   Met risicomanagement kunt u het benodigde beveiligingsniveau vaststellen en daarbij passende maatregelen vaststellen.
   Referenties: hoofdstuk 2.12 en 2.18 van [2], [3], hoofdstuk 6.1 van [5], [16], [18], hoofdstuk 3 van [24].

Checklist organisatorische maatregelen (vervolg)

4. Periodiek vindt een EDP-audit plaats waarin ook de beveiliging van ICS/SCADA-systemen wordt beoordeeld.
   Het is raadzaam om naast de audit periodiek zelfassessments en penetratietesten uit te (laten) voeren.
   Referenties: hoofdstuk 2.16 van [2], [4], [11], hoofdstuk 11 van [24].

5. Er worden beveiligingseisen gesteld die de totale cyclus van ontwikkeling, aanschaf, beheer, onderhoud en vervanging van ICS/SCADA-systemen (hard- en software) afdekken en toepassing van de eisen is gewaarborgd.
   Ook de werkzaamheden die derden uitvoeren en ingekochte producten en diensten moeten aan de beveiligingseisen voldoen. Het is noodzakelijk hiervoor bindende afspraken te maken.
   Referenties: deel 2-4 van [5], [6], [20], hoofdstuk 6 van [24].

6. Periodiek volgen alle medewerkers, ook de medewerkers die met ICS/SCADA-systemen werken, een security-awarenesstraining.
   De mens is een belangrijke schakel in de informatiebeveiliging. Zonder voldoende bewustwording kan elke (technische) maatregel falen. Toets periodiek het awarenessniveau van de medewerkers.
   Referenties: hoofdstuk 2.11 van [2], [10], [19], hoofdstuk 2, 7 en 15 van [24].

7. Wees helder over rollen, taken en verantwoordelijkheden. Maak een team verantwoordelijk voor de beveiliging van ICS/SCADA-systemen. Laat deze medewerkers periodiek aanvullende securitytrainingen volgen. Zorg ook voor betrokkenheid en ondersteuning van de IT-afdeling.
   Eigenaarschap van ICS/SCADA-security is belangrijk. Het moet helder zijn wie waarvoor verantwoordelijk is. Om dit eigenaarschap goed in te kunnen vullen, dienen medewerkers ook over de nodige kennis en vaardigheden beschikken.
   Referenties: hoofdstuk 4.2 van [5], hoofdstuk 2, 7 en 15 van [24].

Checklist technische en operationele maatregelen

1. De ICS/SCADA-systemen maken gebruik van een aparte netwerkinfrastructuur. Deze netwerkinfrastructuur is gescheiden van andere netwerken. De scheiding kan fysiek of logisch zijn ingericht.
   Door gebruik te maken van een aparte netwerkinfrastructuur wordt voorkomen dat (ver)storingen en beveiligingsincidenten in andere netwerken (bijvoorbeeld het standaard kantoornetwerk) direct invloed hebben op de ICS/SCADA-systemen. Wanneer netwerken niet van elkaar zijn gescheiden kan een kwetsbaarheid in het kantoornetwerk bovendien worden misbruikt om toegang te verkrijgen tot de ICS/SCADA-systemen.
   Referenties: [17], [23], hoofdstuk 8 van [24].

2. Beperk koppelingen van ICS/SCADA-systemen met internet en andere netwerken.
   Elke koppeling vormt een potentieel risico. Stel periodiek (minimaal één keer per jaar) een overzicht op van alle koppelingen van uw systemen met internet en andere netwerken. Voer een risicoanalyse uit voor deze koppelingen om de juiste maatregelen te kunnen bepalen. Maak gebruik van beveiligingsapparatuur zoals firewalls, proxyservers en datadiodes en een bijbehorend beleid.
   Er kan een valide reden voor een koppeling zijn, denk bijvoorbeeld aan snelle storingsanalyse, beheer of procesmonitoring. Laat informatie-uitwisseling tussen verschillende netwerken via een apart netwerksegment (DMZ) verlopen. Zorg ervoor dat toegang op afstand alleen plaatsvindt via een centrale beveiligde voorziening en gebruik hierbij tweefactorauthenticatie.
   Referenties: hoofdstuk 2.15 van [2], hoofdstuk 5.8 en 6.3 van [5], Configuring remote access [9], [12], [25].

3. Er is een wachtwoordbeleid opgesteld en er zijn maatregelen getroffen om dit beleid af te dwingen. Onderdeel van dit beleid zijn minimaal:
   - complexiteit van wachtwoorden;
   - wijzigingsfrequentie;
   - wijziging van default accounts en wachtwoorden, inclusief een waarborg voor het verwijderen van dergelijke accounts;
   - eisen ten aanzien van beheersaccounts.

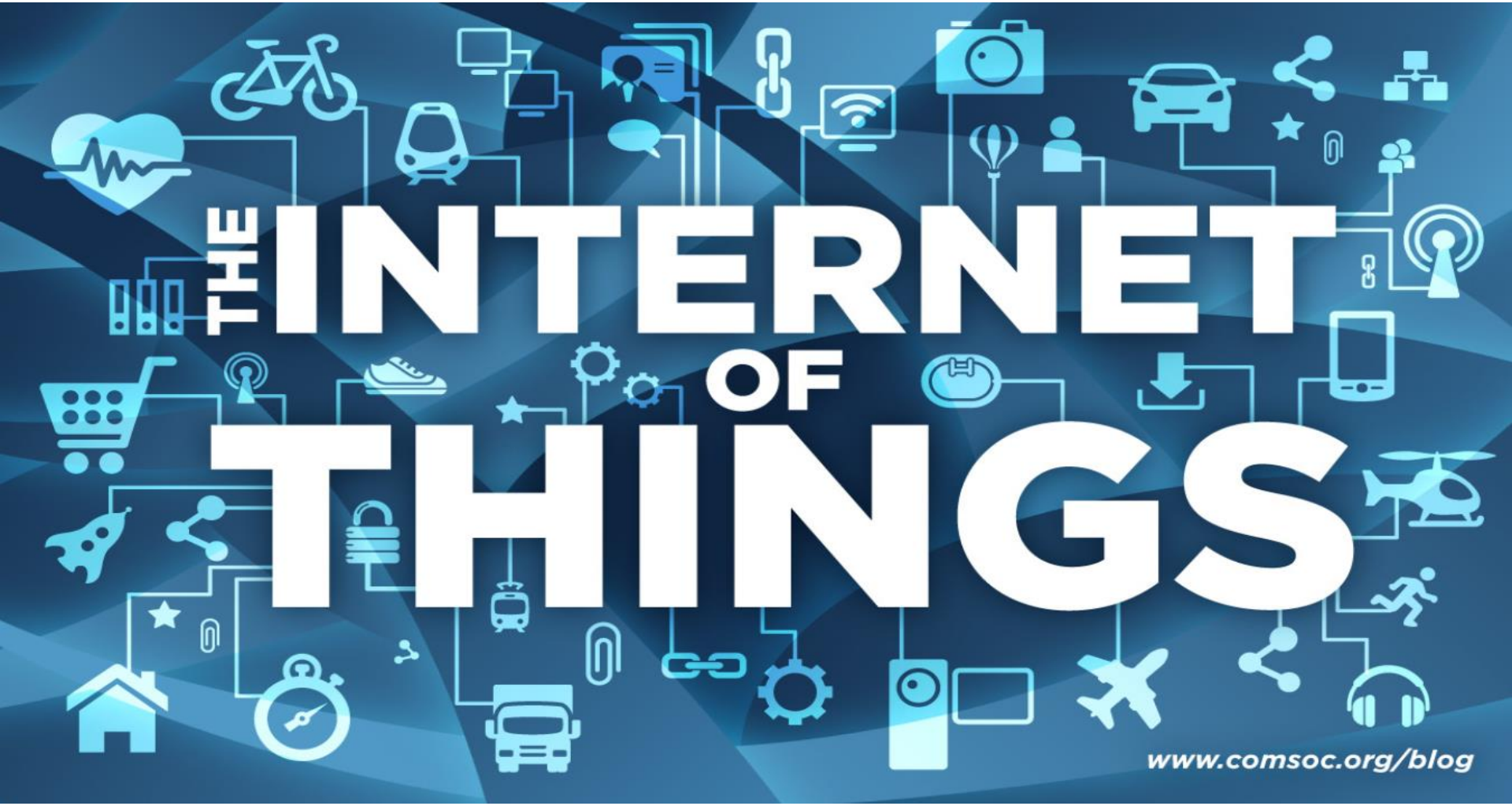
   Wachtwoordbeleid is een groot aandachtspunt bij ICS/SCADA-systemen. Het is echter niet altijd mogelijk om gebruikersaccounts/wachtwoorden te gebruiken. In dergelijke gevallen zullen aanvullende maatregelen, zoals fysieke toegangsbeperkingen, noodzakelijk zijn.
   Referenties: hoofdstuk 2.15 van [2], hoofdstuk 6.3 van [5], hoofdstuk 4.2 van [7].

4. Er is een beleid voor het gebruik van (verwijderbare) media (zoals USB-sticks, harddisks en CD-roms) en er zijn technische maatregelen getroffen om dit beleid af te dwingen.
   Veel virus- en malwareinfecties op ICS/SCADA-systemen worden veroorzaakt door gebruik van besmette opslagmedia. Neem dit beleid expliciet mee in awarenesscampagnes.
   Referentie: hoofdstuk 2.13 van [2], hoofdstuk 6.2 van [5].

PLC: programmable Logic controller - SCADA- Supervisory control and data acquistion

History is about to repeat itself…

Port of Antwerp



PORT TECHNOLOGY

News ▾ Technical Papers ▾

Cybercrime port and shipping industr ‘burden’

21 Oct 2014 09.15am

Lawyers at US law firm Blank Rome have warned that the port and sh industry must take action in combating cybercrime.

According to a statement released by the firm, governments are waking up regarding cyberattack, yet the onus falls on the shipping industry to take th action to prevent them.

Trade Winds reports representatives of Blank Rome as stating: “The failur this responsibility will undoubtedly lead to serious and potentially devastat consequences, including government fines, direct losses, third-party liability, lost customers, and reputational damage that cannot be repaired.

Maersk Freezes Rates After Cyberattack

13 Jul 2017 10.28am

Maersk Group has restored US service contracts data relating which had been temporarily lost in the recent ‘Not Petya’ cyberattack, but earlier this week rates remained frozen as a precautionary measure, according to JOC.com.

Maersk announced on July 11, 2017 that the data had been reclaimed following false reports the data was still inaccessible citing a US Federal Maritime Commission (FMC) public notice.

Maersk corrected the reports, saying it had issued an FMC filing on June 30, 2107 to retain current negotiated container shipping rates as at the time it was "not able to determine which service contracts and/or service contract rates are scheduled to expire at the end of June or in early July."

The attack hit Maersk hard. Its container ships stood still at sea and its 76 port terminals around the world ground to a halt.

In its Crew Connectivity 2015 survey, Futurenautics found that, “Only 12% of crew had received any form of cyber security training. In addition, only 43% of crew were aware of any cyber-safe policy or cyber hygiene guidelines provided by their company for personal web-browsing or the use of removable media (USB memory sticks etc.). Perhaps unsurprisingly, given the above statistics, fully 43% of crew reported that they had sailed on a vessel that had become infected with a virus or malware”.

Maersk hit by another cyber attack

MARCH 19TH, 2018 SAM CHAMBERS EUROPE, OPERATIONS, TECH 2 COMMENTS

Maersk has been hit by another cyber attack. Investigators are looking into how hackers managed to get into towage subsidiary Svitzer Australia’s email system for nearly 10 months before the hack was finally discovered on March 1 this year.

Svitzer officials have stated that the attack has been contained and that it was only limited to the company’s Australian operations, which runs on completely separate systems to the rest of the Maersk Group.

According to Danish shipping news site *Maritime Danmark*, the attack started on May 17 last year when a hidden command in the company’s IT system began to redirect emails to recipients outside Svitzer Australia. The forwarded emails originated from the company’s operating department, financial department and payroll office. The emails were forwarded to two email accounts created on an external server

2

Step 2:

Work on end-user behaviour

ICT Code of conduct

1. Define the purpose
2. Target audience
3. Correct use
4. Incorrect use
5. Responsibilities of the user
6. Use of public networks
7. Repairs
8. Allowed personal usage
9. Password policy
10. How to deal with data and information
11. How to act with social media
12. Monitoring and checks
13. Sanctions
14. ….

CAO 81 - van 26 april 2002

'tot bescherming van de persoonlijke levenssfeer van de werknemers ten opzichte van de controle op elektronische online-communicatiegegevens'

1. Technical incidents

1. Non compliance with the code of conduct
    1. Direct individualisation
    2. Indirect indvidualisation

Approval by the work council makes the code of conduct a binding document for all employees !

Phising and social engineering

Allen voor een groener woon-werkverkeer!

Je kent de campagne ondertussen al: Propere lucht in de haven, daar gaan we voor! Wij willen heel graag het havengebied verder vergroenen, maar zouden nog een stapje verder willen gaan. Om jullie nog meer te stimuleren om de wereld groener te maken, geven we jullie de kans om een elektrische fiets te winnen ter waarde van 4000 euro!!

Klik hier om deel te nemen →

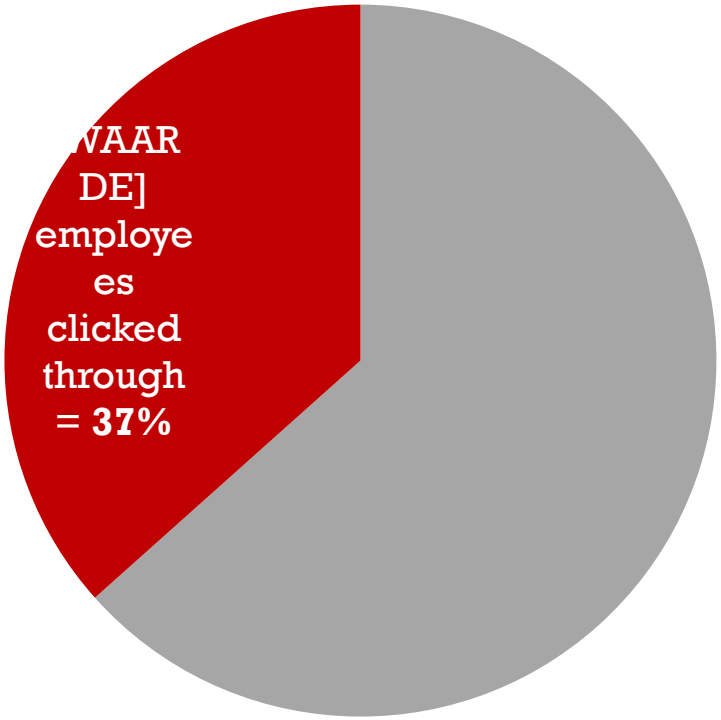
Om dit initiatief op gang te trappen, bieden we jullie de kans een "state of the art" elektrische fiets van Scott te winnen. De perfecte aanzet om meer met de fiets naar het werk te komen! In totaal worden er 10 winnaars geselecteerd. Word jij één van de gelukkigen?

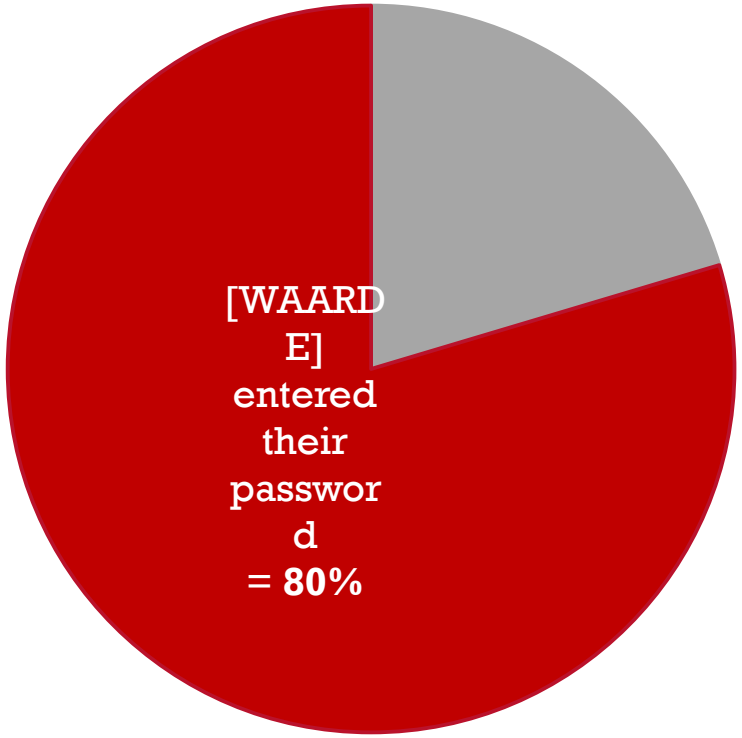
Om deel te nemen aan de wedstrijd, klik je op bovenstaande knop. De wedstrijd loopt nog tot 26 april. De winnaars worden persoonlijk op de hoogte gebracht.

Fiets groener naar je werk met een elektrische fiets!

De Scott E-Spark 720 is een indrukwekkende, elektrische, full suspension MTB met uitstekende rijeigenschappen. Deze fully is klaar voor de strijd: met deze spierbundel kunt u op werkelijk ieder terrein prima uit de voeten! Alles aan deze elektrische MTB van Scott ademt snelheid en plezier! En aangezien deze e-mtb voorzien is van de krachtige Bosch Performance CX motor met een 500 Wh accu, hoeft u niet bang te zijn dat deze fully uw prestaties niet bij kan benen: met de E-Spark gaat u verder en harder dan u ooit hebt gedaan.

Results of an internal phishing campaign*



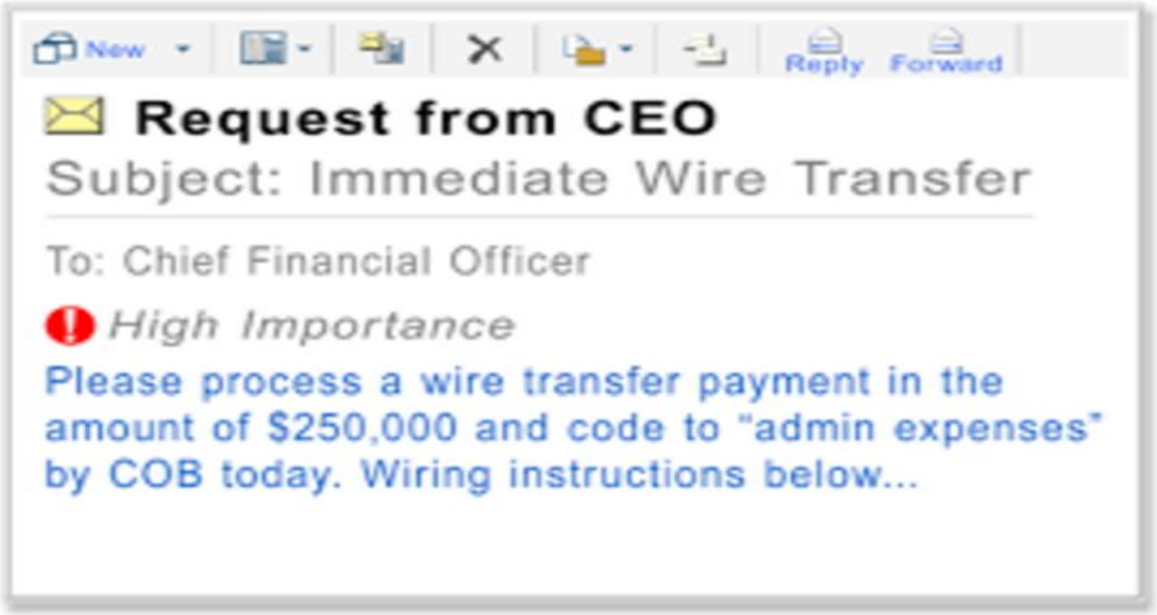


*1702 e-mails sent

Social engineering

How to recognise ?

- Unknown sender
- Urgency
- Offer to good to be true
- Urgent and secret
- Intimidation or flatery



All of this sounds logical, however …

- **46,2%** of all Belgians has a password of **less than 8 characters**
- **33%** of all Belgians **share their password** with others
- **1 out of 4** use the **same password** at home as at work

3

Step 3:

Work on cyber resilience

Cyber resilience – be prepared !

1. Incident handling plan
2. Business continuity plan
3. Keep contact information up to date
4. Report security incidents to C-level
5. Evaluate periodically
6. Identify partners who can help (ISAC)

4

Step 4:

Join a cyber security information sharing network

Information sharing and analysis center: ISAC

Goal of ISAC

- Raise awareness on cybersecurity in the port of Antwerp
- Help each other by exchanging information on new threats and protections in Cyberspace
- Create an early warning system
- Create link between the Port of Antwerp, the port industry and the government

President: Patrick Putman – CIO DP World

4 meetings a year

ISAC@portofantwerp.com

5

How to get started ?

Help is on its way…

CYBER SECURITY COALITION.be

CERT.be

Meer info:

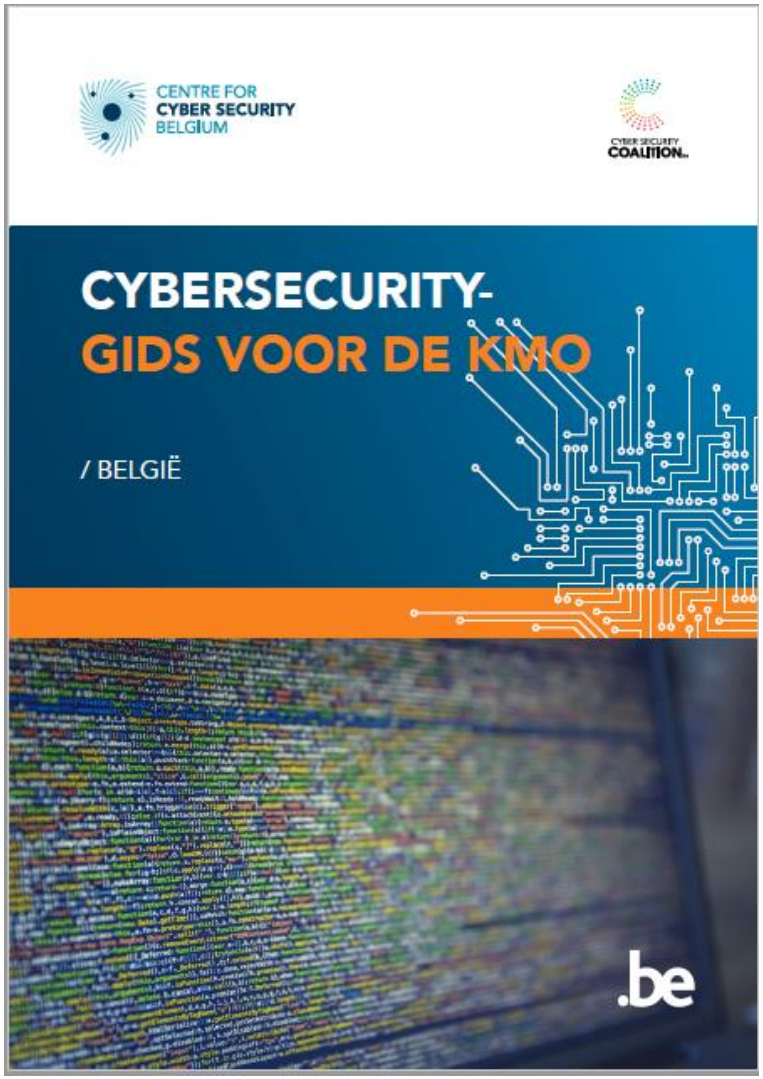
www.cybersecuritycoalition.be

www.safeonweb.be

www.cybersimpel.be

www.safeinternetbanking.be

Cybersecuritycoalition.be



INHOUD

Port of Antwerp

Cyber Security KIT

Released 22 February 2017

Cybersecuritycoalition.be

Our role as port authority

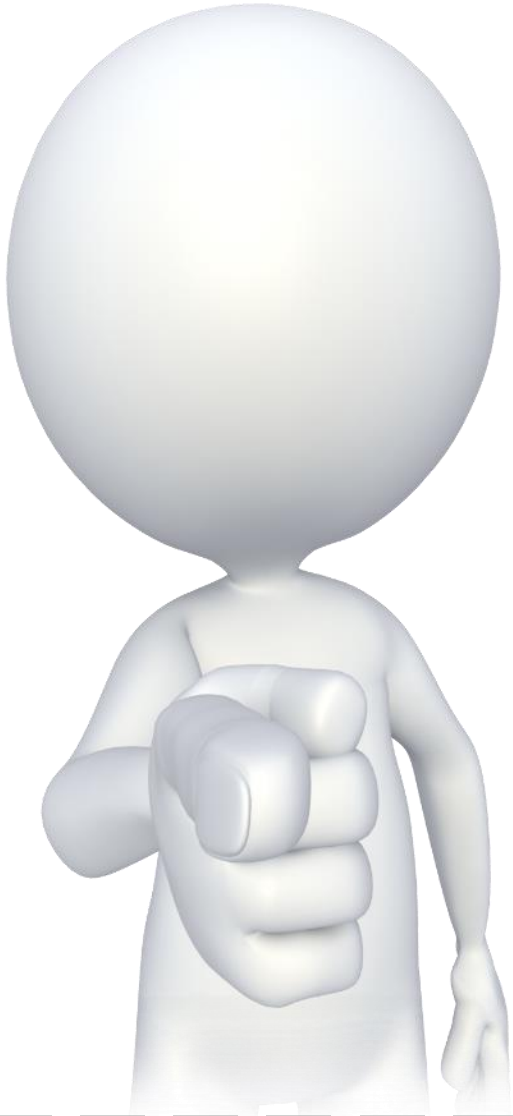
RICHTLIJNEN

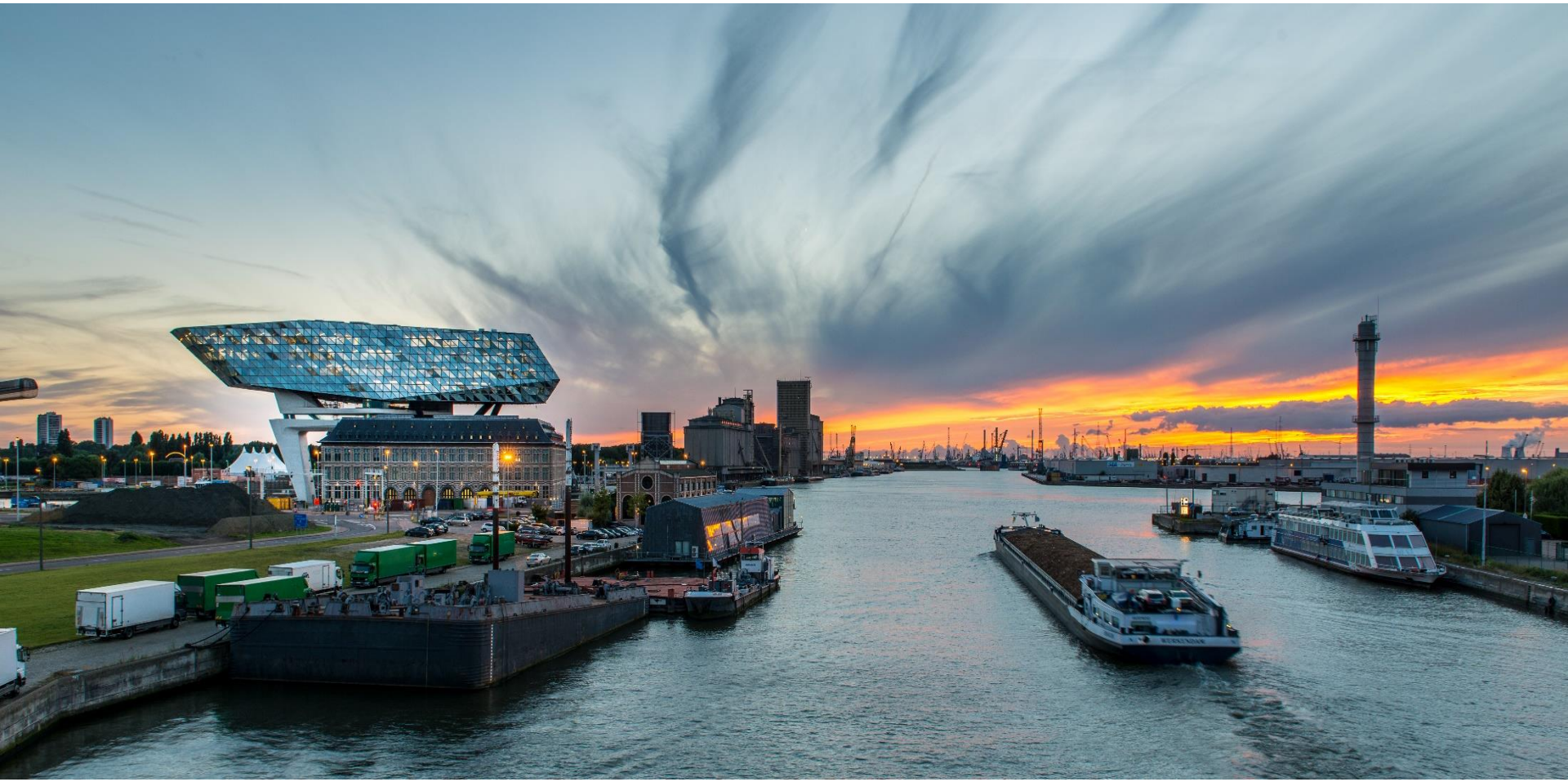
RICHTLIJN (EU) 2016/1148 VAN HET EUROPEES PARLEMENT EN DE RAAD

van 6 juli 2016

houdende maatregelen voor een hoog gemeenschappelijk niveau van beveiliging van netwerk- en informatiesystemen in de Unie

But most of all: BE INVOLVED !





Q & A