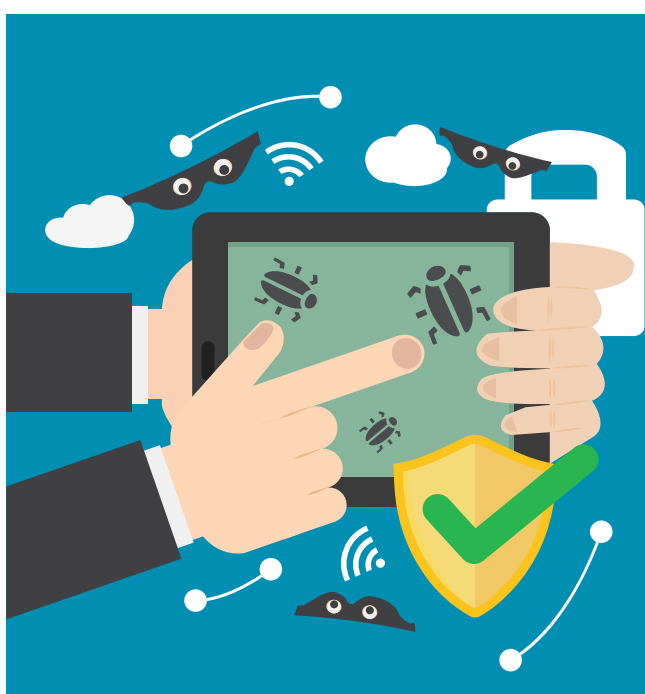


Cyberrisico's in de gezondheidszorg onder controle?

SOCIAL MEDIA

- **39%** van de gebruikers logt niet uit.
- **25%** deelt hun accountinformatie.
- **1** van de **3** gebruikers accepteert uitnodigingen van onbekenden.
- **24%** gebruikt dezelfde online opslag (cloud) prive én zakelijk.
- **12%** van de gebruikers worden gehackt.

TOP RISICO'S IN DE GEZONDHEIDSZORG

1. Ongeautoriseerde toegang (hack of een bekende)
2. Cyberterrorisme
3. Virus of malware
4. Operationele fout
5. Verlies van draagbare media / dataopslagmedium
6. Fysieke schade
7. Coderingsfout
8. Mislukking door leveranciers

(ONTERECHTE) AANNAMES

"Wij hebben geen webshop, dus hebben we ook geen last van cybercrime"

"Wij zijn geen doelwit"

"We voldoen aan alle veiligheidsstandaarden, we zijn dus veilig"

"De bedrijfseconomische risico's van cybercrime vallen wel mee"

"Een firewall beschermt!"

EEN INCIDENT

Wat nu? Hoe organisaties omgaan met cyberrisico's

ONVOORBEREID

- Welke **assets** moeten we beschermen? En hoe?
- Dat is toch iets van **alleen ICT**? Of ligt het ergens anders?
- We deden toch aan **preventie**?
- Wat zijn de **gevolgen** eigenlijk voor onze patiënten?
- Welke **systemen** hebben we en welke **software** gebruiken we?
- Hebben wij een **beleid** voor sterke wachtwoorden, sociale media en/of trainingen op het gebied van online diensten en gedrag?
- Wie is er verantwoordelijk voor de **clouddiensten** die we gebruiken?

ADEQUAAT

Het **cyberincidentplan** treedt in werking:

- uitvoeren van inventarisatie / analyse: wat is de oorzaak (incident of criminaliteit)?
- bepaal de impact van het incident voor:
  - continuïteit
  - veiligheid
  - kwaliteit
  - betrouwbaarheid
  - privacy
  - financiële positie
  - compliance / wet- en regelgeving
  - reputatie

ZIJN ORGANISATIES VOORBEREID OP CYBERINCIDENTEN?

- **77%** had een veiligheidslek in de afgelopen 2 jaar.
- **38%** heeft GEEN cyberincidentplan.
- **17%** vindt dat ze volledig voorbereid zijn op cyberincidenten.
- **41%** denkt dat meer kennis van de risico's en bedreigingen helpt om voorbereid te zijn.
- **57%** rapporteert niet over incidenten als ze daar niet toe verplicht zijn.

DE GEVOLGEN

GROOTSTE BEDREIGING KOMT VAN...

- Hackers 22%
- (Ex-)werknemers 21%
- Andere landen / staten 11%
- Hacktivists 5%
- Georganiseerde misdaad 4%

1

2

3

KOSTEN CYBERCRIME

Wereldwijd
€ 98 miljard per jaar

België
€ 3,5 miljard per jaar

Dagelijks
1 miljoen consumenten slachtoffer

MOGELIJKE IMPACT VOOR DE GEZONDHEIDSZORG

1. Systeemschade
2. Websiteschade / Defacen (ongewild aanpassen van webpagina's door hackers)
3. Dataverlies door derden
4. Elektronische diefstal van uw vertrouwelijke info
5. Lichamelijk letsel / schade aan eigendommen
6. Crisismanagementkosten
7. Reputatieschade
8. Onderzoeken door wetgever en boetes

DE AANPAK: Krijg controle

Stap 1 **Betekenis: wat betekent cyber voor mijn organisatie?**
Inventariseer risico's, bedreigingen en kwetsbaarheden voor uw organisatie.

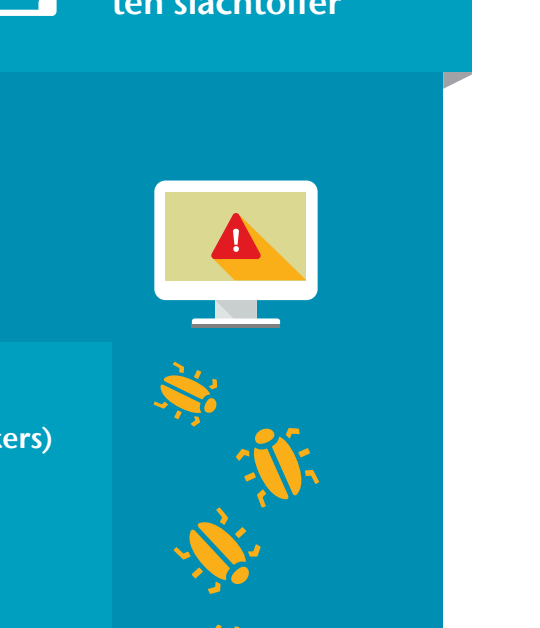
Stap 2 **Consequenties: wat is daarvan de impact?**
Analyseer de mogelijke gevolgen op bedrijfscontinuïteit en -reputatie, mogelijke aansprakelijkheid en schade's en huidige verzekeringsdekking.

Stap 3 **(Beheers)maatregelen: welke maatregelen heb ik of zijn er nodig?**
Bespreek huidige en gewenste maatregelen, implementeer deze en zorg voor adequate borging op de juiste niveaus binnen de organisatie.

Stap 4 **Impact / resultaat: werkt het?**
Bekijk of de genomen stappen het gewenste resultaat / impact hebben, beoordeel of dit voldoende is en stuur waar nodig bij.

QUICK WINS

- Leer van je fouten! Of beter: leer van andermans fouten.
- Cyber is niet een probleem van de IT-afdeling (alleen). Zorg voor een organisatiebrede en samenhangende aanpak.
- Beoordeel in hoeverre de organisatie weerbaar is en veerkracht heeft tegen ICT-gerelateerde incidenten.
- Zorg voor bewustzijn, bijvoorbeeld door trainingen.
- Zorg voor gedegen updatebeleid & onderhoud van systemen.
- Monitor constant de eigen essentiële ICT-infrastructuur.



Zorg voor bewustzijn en maak beleid

Bronnen
- Persbericht, Cyber Security Coalition, Oktober 2014
- Underrated Threats Report, Aon plc, 2013
- Cyberrisico's managen met de Aon-aanpak, Aon Groep Nederland, 2013
- General Threat Landscape, Mandiant, 2013
- Cyber incident response: Are business leaders ready?, The Economist, Intelligent Unit, 2014
- Net Losses: Estimating the Global Cost of Cybercrime, McAfee, 2014
- Cost of Cyber Crime Study: Global Report, Ponemon Institute, October 2013
- Norton Report, Symantec, 2013
- Are you making yourself victim of Cybercrime?, Zone Alarm, June 2014
- ENISA Threat Landscape, Responding to the Evolving Threat Environment, September 2014

Hoe staat uw organisatie er voor?
Gebruik de diagnosetool.
Kijk op **aon.be/cyber**

1023-cyber14-BE-NL-Gezondheidszorg-v2

Risk. Reinsurance. Human Resources.

AON
Empower Results®