Secundity

Cybersecurity & ethisch hacken

Hoe veilig is jouw laboratorium?

Sijmen Ruwhof
Cybersecurityspecialist & Ethisch Hacker

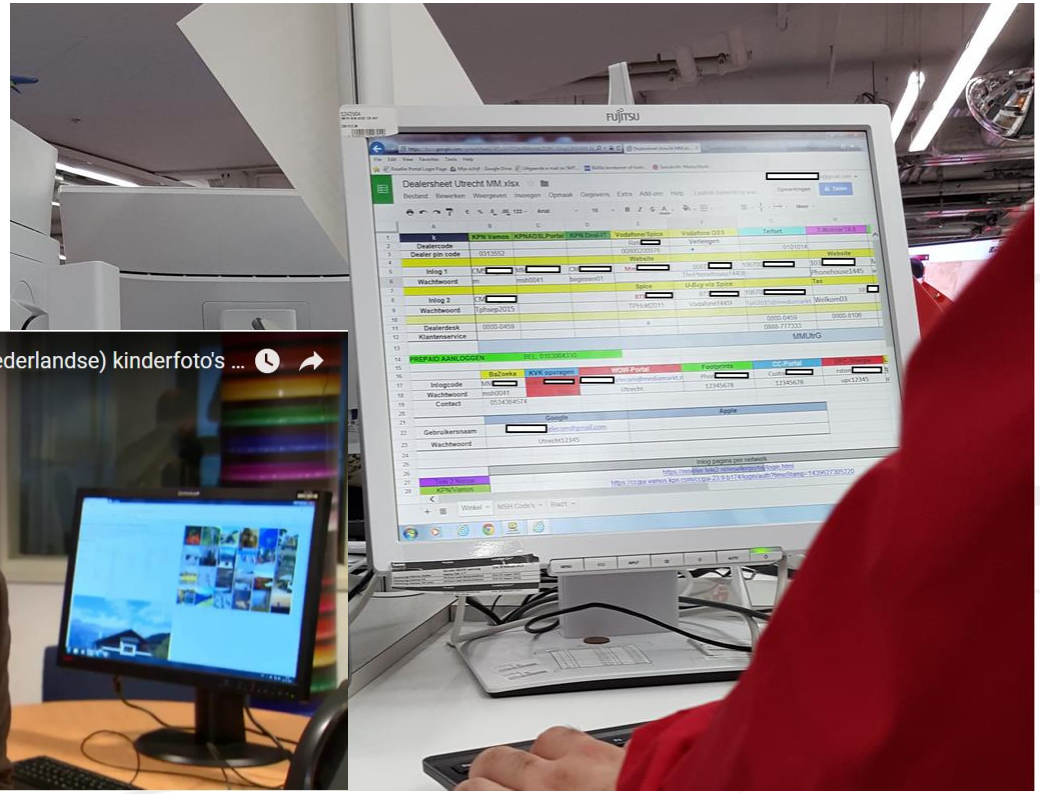
Wie ben ik?

Secundity

- Gestart met hacking in 1997 : 26 jaar
- Sinds 2005 professioneel : 18 jaar
- 700+ beveiligingstesten uitgevoerd voor 100+ bedrijven

Bedrijven waar ik zoal voor werk

In de media



Weblog: https://sijmen.ruwhof.net

rtlnieuws

Met potlood stemmen onveilig: verkiezingsuitslag eenvoudig te hacken

Secundity

30 januari 2017 17:48

Het stembureau in de boksschool aan de Amsterdamse Albert Cuijpstraat.

We gebruiken al jaren het rode potlood, maar achter de schermen worden alle stemmen geteld door software. Dit systeem is zo lek als een mandje, waardoor hackers de uitslag van de verkiezingen kunnen manipuleren.

rtl nieuws

Vrees voor hackers: kabinet schrapt software, stemmen tellen volledig met de hand

01 februari 2017 17:55

De stemmen worden voortaan volledig met de hand geteld.

Bij de aankomende Tweede Kamerverkiezingen worden alle stembiljetten weer met de hand bij elkaar opgeteld. Het kabinet trekt na berichtgeving van RTL Nieuws de stekker uit de onveilige software waarmee al acht jaar lang de uitslag van de verkiezingen wordt berekend.

Wat niet in het nieuws komt

Secundity

- Resultaten van 700+ uitgevoerde beveilingstesten:
  - In 80-90% van de testen hoog beveiligingsrisico
  - In 20% zelfs kritisch beveiligingsrisico (!)
  - Gemiddeld 1 tot 2 beveiligingsrisico's per testuur
  - Vaak staat software al jaren in productie
  - Vaak pas testen als al is ingebroken of pas als klant er om vraagt

Inleiding

Secundity

- De snelle opkomst van software
- Datalekken, en de oorzaken
- Cybercrime
- Cyberwarfare
- Cybersecurity
- Hoe ons voorbereiden en verder?

De snelle opkomst van software

Software-ontwikkeling

Secundity

- Projectleider vraagt IT-bedrijf om software te ontwikkelen
- IT-bedrijf levert software op
- Klant voert acceptatietest uit: *“Ziet er goed uit!”*

Software-ontwikkeling

- Discrepantie wens klant en interpretatie IT-bedrijf
  - IT-bedrijf haalt planning niet
  - Project gaat over budget heen
- Uitgangspunt: IT-bedrijf wil winst maken
  - Programmeurs weer snel op volgend project gezet na oplevering

Trends

- Digitalisering
- Centralisering
- Schaalvergroting en mondialisering
- Vergroting complexiteit
- Aansluiting op internet
- Automatisering en kostenreductie
- Specialisatie en uitbesteding

De markt volgt de techniek

- De techniek gaat zeer snel vooruit
- De markt wil daarvan profiteren, en ook:
  wie niet mee gaat, verliest de strijd
- Automatiseren werkt zeer kostenbesparend
- Bijna niemand bewust van beveiligingsrisico’s
- Veel oude infrastructuur en achterstallig onderhoud
- Beveiliging is onzichtbaar

Lekken worden niet gedicht

- Geen overzicht van gebruikte ICT-infrastructuur:
  - Geen of onvolledige administratie
- Veel assets niet in beheer:
  - Na initieel in productie zetten, nooit meer onderhouden
- Updaten en testen te duur
- Apparatuur kan niet eenvoudig geüpdatet worden
- Ernst van lek niet begrepen


YOU HAVE BEEN HACKED

Criminelen leggen Belgisch lab dat coronatests uitvoert plat en eisen losgeld

Criminele hackers hebben het operationele systeem van het Algemeen Medisch Laboratorium in het Belgische Hoboken platgelegd. Het laboratorium voert per dag zo'n 3000 coronatests uit, wat neerkomt op vijf procent van het landelijk totaal.

Volgens de Gazet van Antwerpen vragen de hackers om losgeld om de systemen weer werkend te maken, maar het laboratorium zegt daar niet op ingegaan te zijn. In plaats daarvan is het naar de autoriteiten gestapt. De Belgische Computer Crime Unit heeft een onderzoek in gang gezet. Er lijken geen patiëntengegevens gestolen te zijn bij de inbraak, zeggen de betrokken partijen. De systemen bij het Algemeen Medisch Laboratorium liggen door de hack sinds maandag 28 december stil.

Het is niet de eerste keer dat een instantie die zich bezighoudt met de bestrijding van het coronavirus het doelwit is van een hack. Begin december was het Europees Geneesmiddelenbureau EMA, dat de coronavaccins van Pfizer/BioNTech en Moderna moest keuren, het doelwit van een digitale aanval. De aanvallers hadden toegang tot de documenten over de werking van het vaccin. Ook waren de aanvallers op zoek naar informatie over de toelatingsprocedures van de vaccins en over betrokkenen bij de onderzoeken daarmaar. Het is niet duidelijk of ze die informatie ook hebben weten te bemachtigen.

Bron (29-12-2020): https://tweakers.net/nieuws/176192/criminelen-leggen-belgisch-lab-dat-coronatests-uitvoert-plat-en-eisen-losgeld.html

Buitenlandse inlichtingendienst zat waarschijnlijk achter EMA-hack

Een digitale aanval op het Europees Geneesmiddelenbureau EMA, waarbij informatie over de werking van vaccins is ingezien, was waarschijnlijk geen toevalstreffer. De aanvallers lijken gericht naar die informatie op zoek te zijn geweest.

De Duitse regionale omroepen WDR en BR melden dat het om een buitenlandse inlichtingendienst lijkt te gaan. Een bron van de NOS bevestigt die lezing. Om welke overheid het gaat, is niet duidelijk.

Volgens de bron werd de hack ontdekt toen een medewerker op ongebruikelijke tijden ingelogd was op een server van het EMA. Zijn account bleek te worden misbruikt door de aanvallers. Die lezing wordt bevestigd door de Duitse omroepen.

Bron (23-12-2020): https://nos.nl/artikel/2361735-buitenlandse-inlichtingendienst-zat-waarschijnlijk-achter-ema-hack

Gehackt systeem voor onderdruk

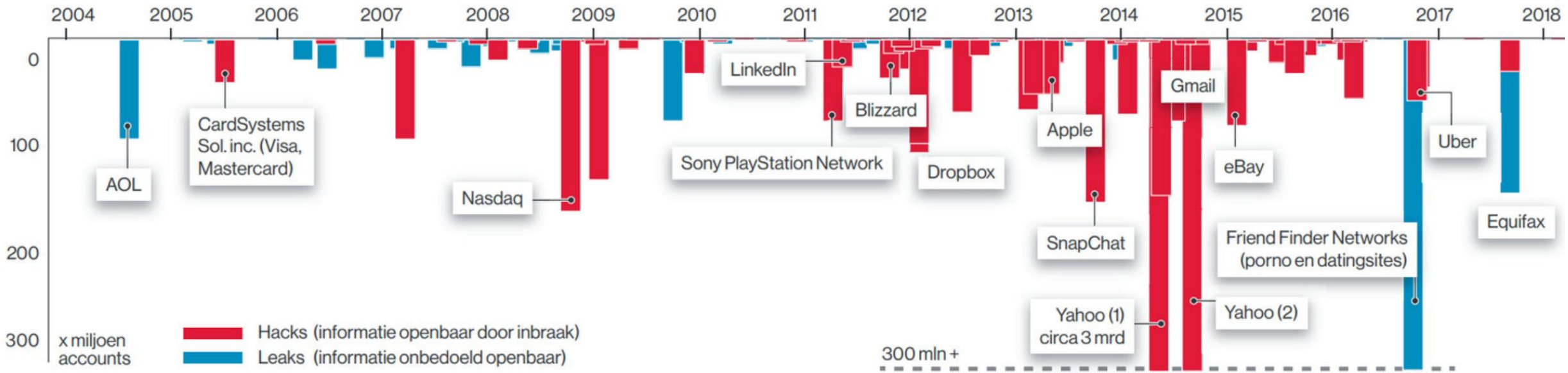
Bij dual-use denk je wellicht aan onderzoek aan hoogrisico pathogenen, maar heb je er ooit bij stil gestaan dat dual-use onderzoek ook plaats zou kunnen vinden binnen de informatica-afdeling van een universiteit/onderzoekscentrum? Vorige week verscheen een nieuwsbericht dat aandacht besteedt aan een recent gepubliceerd onderzoek dat tot in detail beschrijft hoe een onderdruksysteem in een biologisch laboratorium gehackt kan worden.

Het scenario: gehackt systeem voor onderdruk

Binnen een grote Amerikaanse universiteit is een onderzoek uitgevoerd naar de mogelijkheid om onderdruksystemen in biologische laboratoria te hacken. Het team ontregelde niet alleen het systeem in een echt laboratorium, maar de onderzoekers legden ook tot in detail uit hoe de hack moest worden uitgevoerd. Hoewel het aanpakken van mazen in

Bron (25-01-2023): https://www.bureaubiosecurity.nl/nieuws/biosecurity-scenario-gehackt-systeem-voor-onderdruk

Datalekken


2004
2005
2006
2007
2008
2009
2010
2011
2012
2013
2014
2015
2016
2017
2018
0
100
200
300
x miljoen accounts
AOL
CardSystems Sol. inc. (Visa, Mastercard)
Nasdaq
LinkedIn
Sony PlayStation Network
Blizzard
Dropbox
Apple
SnapChat
Gmail
eBay
Yahoo (1) circa 3 mrd
Yahoo (2)
Friend Finder Networks (porno en datingsites)
Uber
Equifax
300 mln +
Hacks (informatie openbaar door inbraak)
Leaks (informatie onbedoeld openbaar)

Meest gelekte wachtwoorden

Verander nu je wachtwoord: 3,3 miljoen Nederlandse wachtwoorden eenvoudig te vinden

VIDEO'S | **Een grote hoeveelheid e-mailadressen en 3,3 miljoen wachtwoorden van Nederlanders liggen op straat. Ze blijken sinds eind vorig jaar betrekkelijk eenvoudig in te zien in lijsten die online circuleren. Een hacker maakt ze vandaag via een speciale zoekmachine zelfs nog toegankelijker: een 'Google' voor wachtwoorden.**

Gelekte accounts per instelling

Secundity

Financiële instellingen	
ing.nl	3475
rabobank.nl	2032
achmea.nl	1680
interpolis.nl	642
nn.nl	496

Media	
telegraaf.nl	205
nos.nl	200
vpro.nl	196
ad.nl	191
rtl.nl	184

Overheden	
uwv.nl	2534
rws.nl	1611
mindef.nl	1268
minbuza.nl	1213
minlnv.nl	968
utrecht.nl	673
minvrom.nl	636
minjus.nl	594
denhaag.nl	550
brabant.nl	457
minbzk.nl	436

Onderwijsinstellingen	
uva.nl	4225
rocwb.nl	3634
wur.nl	3144
uu.nl	2879
tudelft.nl	2601
inholland.nl	2166
rug.nl	2026
hva.nl	2017
erasmusmc.nl	1582
uvt.nl	1357

';--have i been pwned?

Secundity

Largest breaches

- 772,904,991 Collection #1 accounts
- 763,117,241 Verifications.io accounts
- 711,477,622 Onliner Spambot accounts
- 622,161,052 Data Enrichment Exposure From PDL Customer accounts
- 593,427,119 Exploit.In accounts
- 509,458,528 Facebook accounts
- 457,962,538 Anti Public Combo List accounts
- 393,430,309 River City Media Spam List accounts
- 359,420,698 MySpace accounts
- 268,765,495 Wattpad accounts

717
pwned websites

12,750,394,100
pwned accounts

115,763
pastes

228,881,458
paste accounts

';--have i been pwned?

Check if you have an account that has been compromised in a data breach

email address pwned?

Oorzaken

- IT-beveiliging is onzichtbaar, totdat het misgaat.
- Klant kan status beveiliging niet beoordelen.
- Ontwikkelaars focussen op functionaliteit, niet veiligheid.
- Hoger management niet bewust en bekend met veiligheidsrisico’s.

De echte oorzaak

- Awareness, kennis en budget

- Beveiliging kost geld en is niet omzet verhogend
- Echter, beveiligingsincident is vele malen duurder

ndity

Nieuwe wetgeving

- **2016-01:** Meldplicht datalekken
- **2018-05:** Algemene Gegevensverordening (AVG/GPDR)
  - Strenge nieuwe EU-wetgeving.
  - Tot 20 miljoen euro boete, of tot 4% van wereldwijde omzet.
- **2019-01:** Wet beveiliging netwerk- en informatiesystemen
  - Zorg- en meldplicht datalekken voor kritische infrastructuur.
- **2024?:** Network and Information Security (NIS2) directive
  - Zorg- en meldplicht, toezicht

Cybercrime kan zeer lucratief zijn

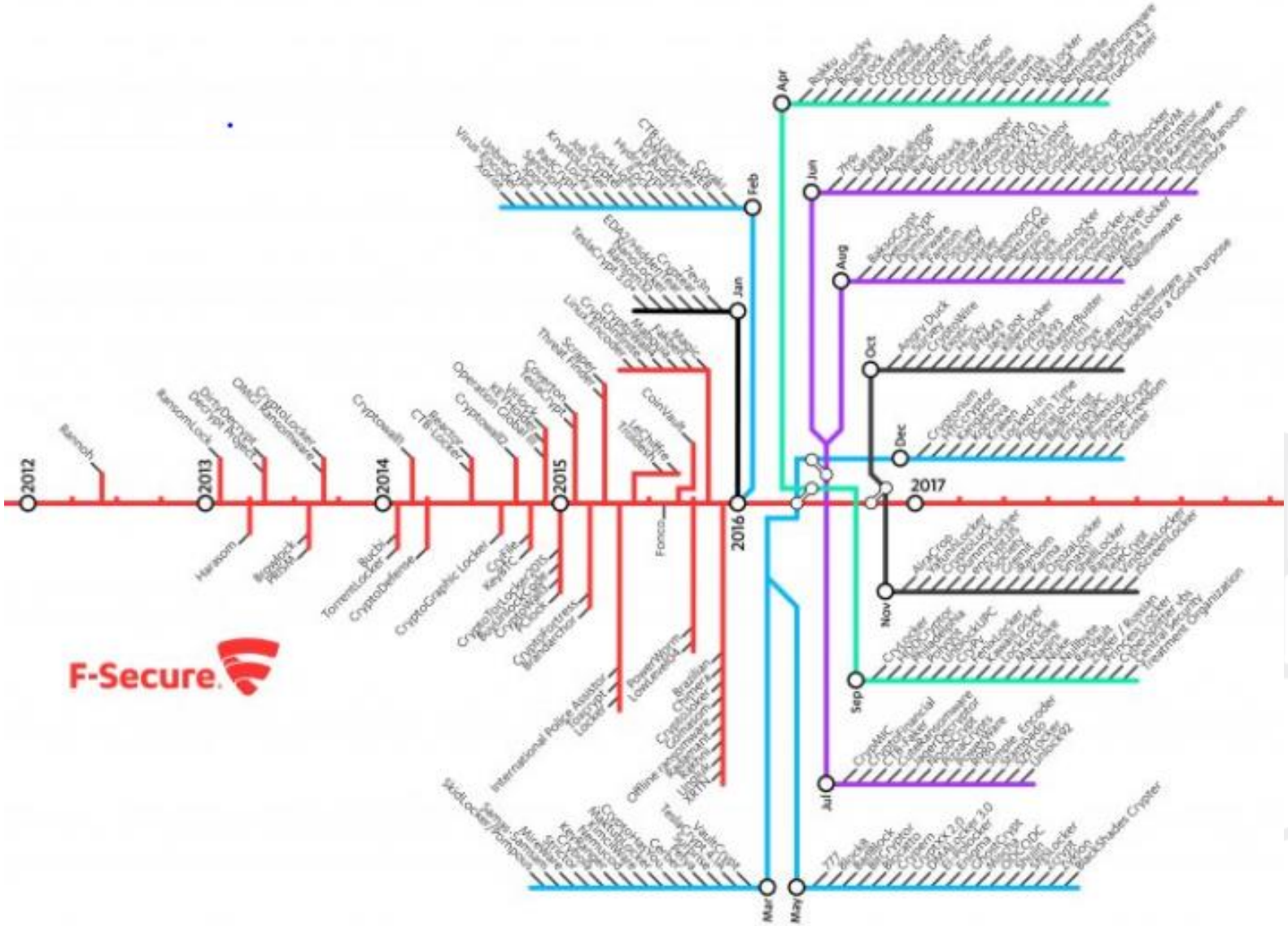
Botnets


trojan
rootkit
worm
ransomware
virus
spyware


Malware
ed webpage
Outdated Plugin
BACKDOOR
OTHER ZOMBIE PC'S
BACKDOOR
YOUR ZOMBIE PC
BACKDOOR
MORE ZOMBIE PC'S
COMMAND-AND-CONTROL SERVER
Powerful attacks
SPAM, DOS, PHISHING, RANSOMWARE, CLICK FRAUD ETC.

Ransomware is booming

Secundity



Ooops, your files have been encrypted!

English

Payment will be raised on

5/16/2017 00:47:55

Time Left

02:23:57:37

Your files will be lost on

5/20/2017 00:47:55

Time Left

06:23:57:37

What Happened to My Computer?

Your important files are encrypted.
Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?

Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.
You can decrypt some of your files for free. Try now by clicking <Decrypt>.
But if you want to decrypt all your files, you need to pay.
You only have 3 days to submit the payment. After that the price will be doubled.
Also, if you don't pay in 7 days, you won't be able to recover your files forever.
We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?

Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.
Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.
And send the correct amount to the address specified in this window.
After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am

bitcoin ACCEPTED HERE

Send $300 worth of bitcoin to this address:

12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw

Copy

About bitcoin

How to buy bitcoins?

Contact Us


Login
Password

Van: postnl@postnl-tracktrace.com [mailto:postnl@postnl-tracktrace.com]
Verzonden: dinsdag 14 oktober 2014 15:15
Aan:
Onderwerp:[NAAM ONTVANGER] heb je niet geleverde pakket

Track & Trace

[NAAM ONTVANGER]

Een koerier had het pakket niet leveren aan uw adres 9 oktober 2014, omdat niemand thuis was.
Zie de informatie over uw pakket, print het uit en ga naar het postkantoor om uw pakket te ontvangen.

Aandacht!

http://creaturainferno.ru/.projects/usbms/wp-content/uploads/2014/08/showthread.php?id=8350726115

Als het pakket niet binnen 30 dagen is ontvangen dan PostNL heeft het recht om schadeloosstelling vorderen van u voor het is houden van in het bedrag van 4,55 euro voor elke dag van het houden!

Deze automatisch gegenereerde e-mailbericht. Klik hier om af te melden.

Gevolgen

- Imagoschade
- Veel geld verloren
- Datalek en -verlies
- Verlies aan klanten en omzet, faillissement
- Onbereikbaarheid (DDoS)
- Boetes en rechtzaken, betrokkenheid toezichthouder
- Afpersing
- *Bestuurders persoonlijk aansprakelijk*


CYBER WARFARE

Cyber leger

- Ruim 30 landen hebben toegegeven een militaire cyberdivisie te hebben
- De laatste 15 jaar zijn veel cyberwapens gecreëerd
- Internet wordt laatste jaren snel gemilitariseerd
- Krachtige cyberwapens liggen regelmatig op straat

NATIONAL SECURITY AGENCY

UNITED STATES OF AMERICA

IMAGE VIA COLIN / WIKIMEDIA COMMONS

China

- Joint Striker Fighter
- Onderzeeërs
- Zeer ervaren in spionage
- Huawei / ZTE

Noord Korea

- WannaCry
- Bangladesh bank
- Sony


RISE OF THE
HACKERS
Source: Carna Botnet

Verschillende soorten hackers

Actor	Intentie	Vaardigheids-niveau	Doelwit
Staten	Voor contraterrorisme of bescherming Nationale Veiligheid Geopolitieke of (interne) machtspositie verbeteren	Hoog	Overheidsinstellingen, defensie-industrie en bedrijven in topsectoren. Organisaties die springplank vormen om anderen te 'targeten'
Terroristen	Maatschappelijke veranderingen bewerkstelligen, bevolking ernstige vrees aanjagen of politieke besluitvor-ming beïnvloeden	Gemiddeld tot laag	Doelwitten met hoge impact, ideologische symboolfunctie
Beroepscriminelen	Geldelijk gewin (direct of indirect)	Hoog tot gemiddeld	Producten en –dienstverlening met veel identiteits- of financiële gegevens In beginsel iedereen waar op illegale wijze geld aan te verdienen is
Cybervandalen en scriptkiddies	Baldadigheid, zoeken van uitdaging	Laag	Uiteenlopend

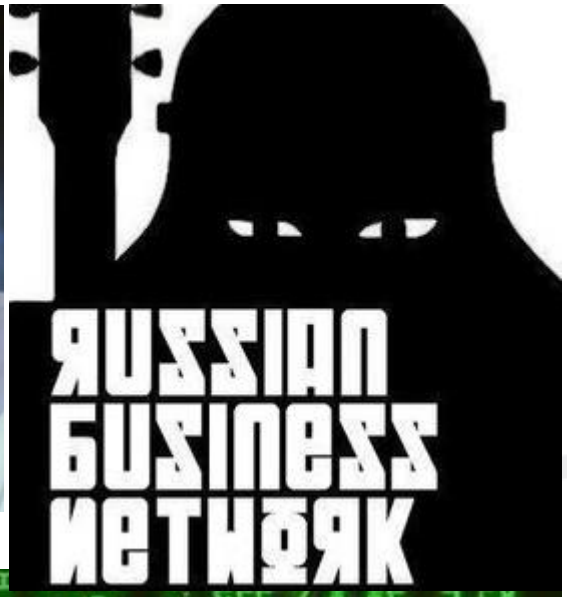
Verschillende soorten hackers

Secundity

Hacktivisten	Ideologische doelen dichterbij brengen	Gemiddeld	Nieuwsorganisaties. Gerelateerd aan ideologisch doel dat wordt nagestreefd. Soms ook totaal willekeurig met als enige reden aanwezige kwetsbaarheden
Interne actoren	Wraak, geldelijk gewin of ideologisch (mogelijk 'aangestuurd')	Hoog tot laag	Huidige en/of voormalige werkomgeving
Cyberonderzoekers	Aantonen zwakheden, eigen profilering	Gemiddeld	Uiteenlopend
Private organisaties	Verkrijging of verkoop waardevolle informatie	Hoog tot laag	Concurrenten, burgers, klanten

Voorbeelden van hackers

Secundity



Dreigingen

Bron van Dreiging	Overheden	Private organisaties	Burgers
Staten	Digitale Spionage	Digitale Spionage	Digitale Spionage
	Offensieve cybercapaciteiten	Offensieve cybercapaciteiten	
Terroristen	Verstoring/overname ICT	Verstoring/overname ICT	
Beroepscriminelen	Diefstal en publicatie of verkoop van informatie ↓	Diefstal en publicatie of verkoop van informatie	Diefstal en publicatie of verkoop van informatie ↑
	Manipulatie van informatie ↓	Manipulatie van informatie ↓	Manipulatie van informatie
	Verstoring ICT ↑	Verstoring ICT ↑	Verstoring ICT ★
	Overname ICT ↓	Overname ICT ↑	Overname ICT
Cybervandalen en scriptkiddies	Diefstal informatie ↓	Diefstal informatie ↓	Diefstal informatie
	Verstoring ICT ↓	Verstoring ICT	

Dreigingen

Bron van Dreiging	Overheden	Private organisaties	Burgers
Hacktivisten	Diefstal en publicatie verkregen informatie	Diefstal en publicatie verkregen informatie	Diefstal en publicatie verkregen informatie
	Defacement	Defacement	
	Verstoring ICT	Verstoring ICT	
	Overname ICT ★	Overname ICT	
Interne actoren	Diefstal en publicatie of verkoop verkregen informatie	Diefstal en publicatie of verkoop verkregen informatie	
	Verstoring ICT	Verstoring ICT	
Cyberonderzoekers	Verkrijging en publicatie van informatie	Verkrijging en publicatie van informatie	
Private Organisaties		Diefstal informatie (bedrijfsspionage) ↓	Commercieel ge-/misbruik of 'doorverkopen' gegevens ★
Geen actor	Uitval ICT	Uitval ICT	Uitval ICT

Cybersecurity

Hoe ons voorbereiden?

- Bewustzijn vergroten
- Kennis opdoen
- Vooruit kijken:
  - Dreigingen
  - Veiligheidsrisico’s

Hoe ons voorbereiden?

Secundity

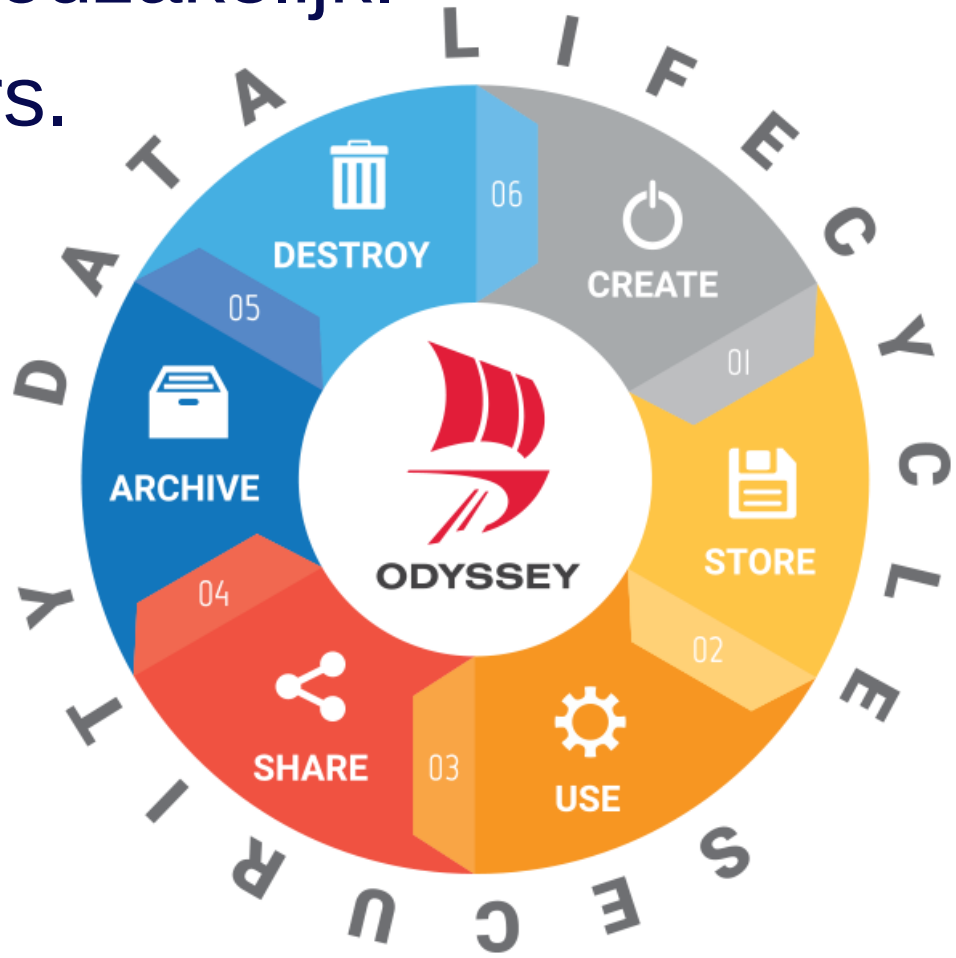
- Voorkom lekken:
  - Betrek security experts bij software ontwikkeling
  - Security- en privacy-by-design
  - Laat ethische hackers de software testen
- Goed en strak IT beheer.
- Richt security monitoring in:
  - Intrusion detection & prevention
  - Tuning! En adequate opvolging

Security-by-design

- Risicoanalyses.
- IT security experts betrekken.
- Architectuur en ontwerp laten reviewer
- Regelmatig pentesten uitvoeren.
- Gerichte security monitoring.
- Vulnerability management.

Privacy-by-design

- Niet meer informatie opslaan dan noodzakelijk.
- Verwijder oude informatie en dossiers.
- Encryptie.



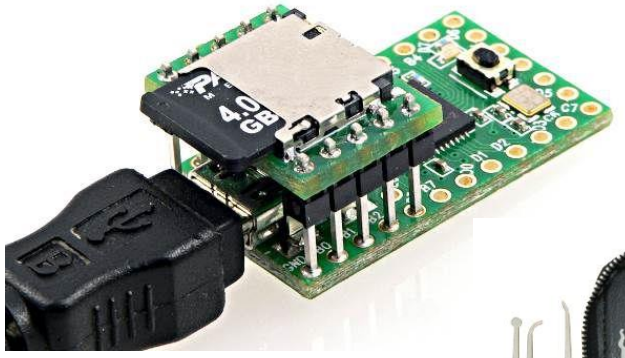
Security Operations Centers

Inbraakdetectie
Inbraakpreventie
Logging
Monitoring
Incident response


THE POWER OF
RED TEAMING

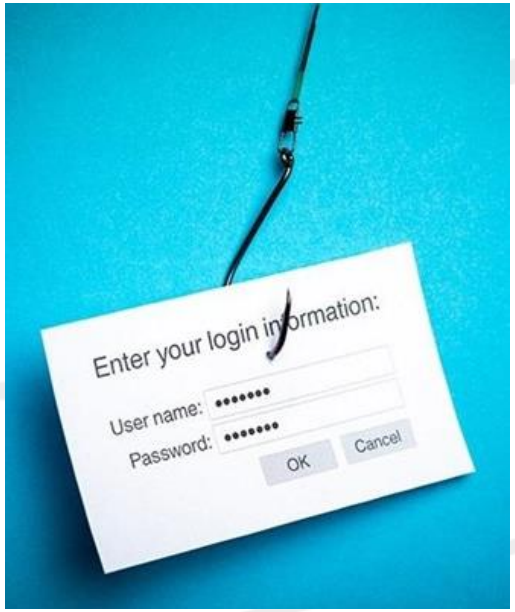
Hacker gear: hardware

Secundity



Hacker gear: soft skills

Secundity



Uitdagingen

- Eindgebruikers blijven de zwakste schakel
- Social engineering kan elke security maatregel omzeilen
- Bijna iedereen trapt in een spear phishing mail
- Security monitoring bijna nooit (goed) ingericht
- Groot tekort aan technische cyber security specialisten
- Managementaandacht voor cyber security verslapt snel
- Weinig budget, tijd en aandacht voor security

Cybersecurity hygiene

- Updates altijd snel installeren
- Unieke en sterke wachtwoorden (wachtwoordmanager)
- Configuratie-opties altijd regelmatig nalopen
- 2FA instellen


The battle is on!

Sijmen Ruwhof

sijmen@ruwhof.net

sijmen.ruwhof.net

twitter.com/sijmenruwhof