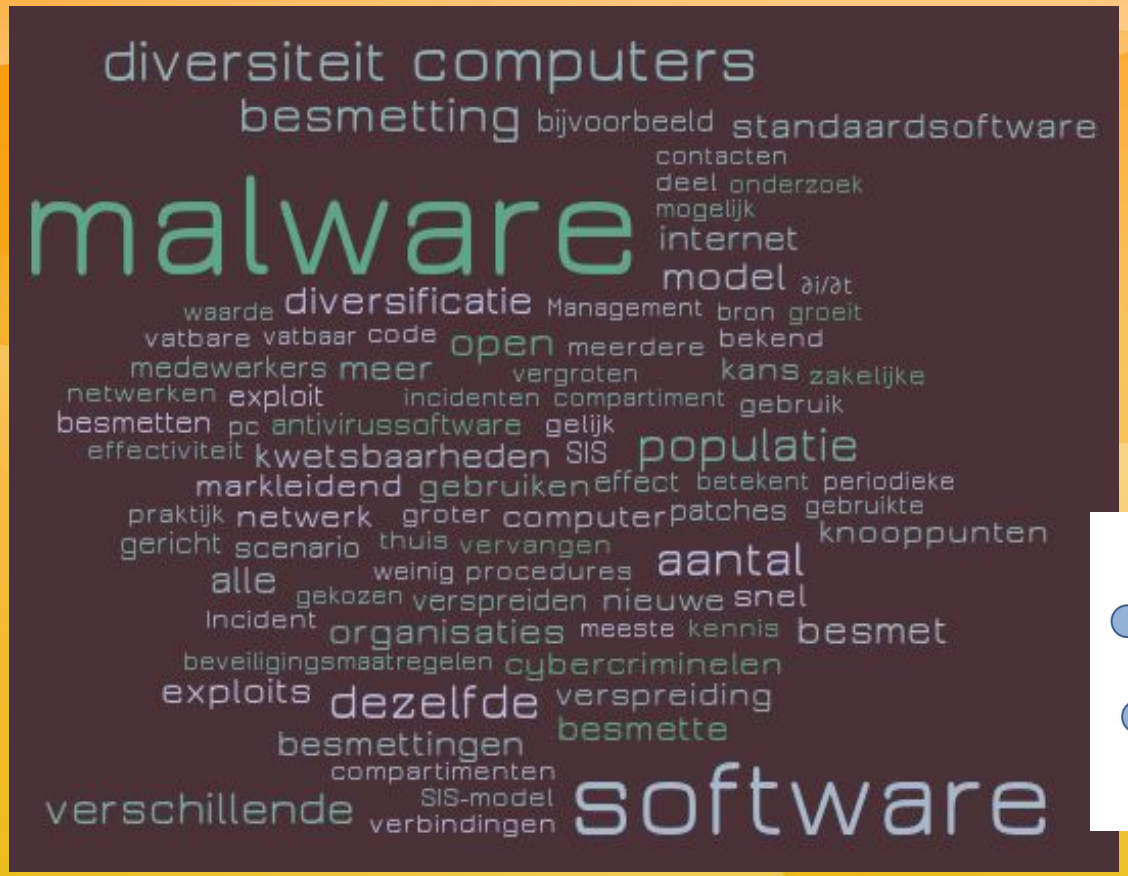
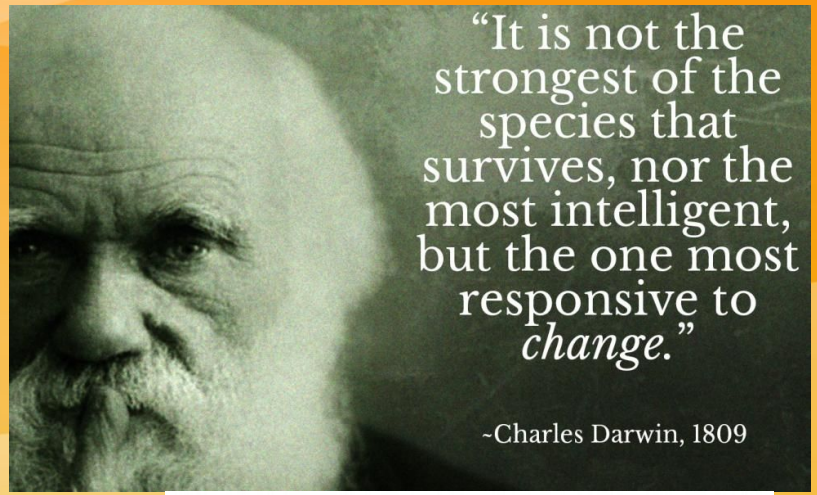
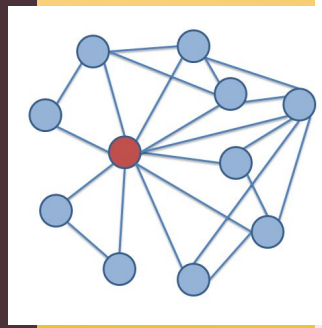
Hogere weerbaarheid met ICT diversiteit







Even voorstellen… Henk-Jan van der Molen

1961

1984

DMR Consulting

1998

Inspectie Leefomgeving en Transport
Ministerie van Infrastructuur en Waterstaat

2006

Ministerie van Volksgezondheid, Welzijn en Sport

2019

1979

$$\mathcal{F}(\omega) = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{\infty} f(t) e^{-i\omega t}\,\mathrm{d}t$$

1990

2002

SZW

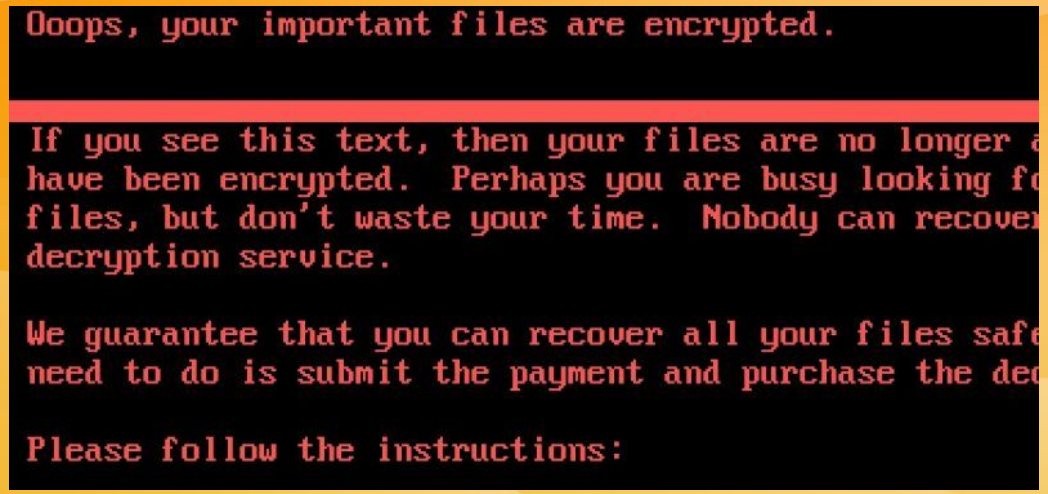
2013

Ministerie van Veiligheid en Justitie

RAAD VOOR ACCREDITATIE

SECURITY ACADEMY

Oorzaak van Wannacry en NotPetya?



NotPetya Ransomware Attack Cost Shipping Giant Maersk Over $200 Million

Lee Mathews Contributor 7,480 views #CyberSecurity

In June, the NotPetya ransomware hit companies in the U.S. and throughout Europe. One of those hardest hit was Copenhagen-based shipping giant A.P. Moller-Maersk, which moves about one-fifth of the world's freight. Operations at Maersk terminals in four different countries were impacted, causing delays and disruption that lasted weeks.

Now that the dust has finally settled, Maersk has revealed the financial impact the NotPetya attack had. According to a statement issued by the company, the total cost for dealing with the outbreak will land somewhere in the $200 to $300 million range. NotPetya-related costs contributed to a $264 million quarterly loss despite revenues rising from $8.7 billion to $9.6 billion year-over-year.

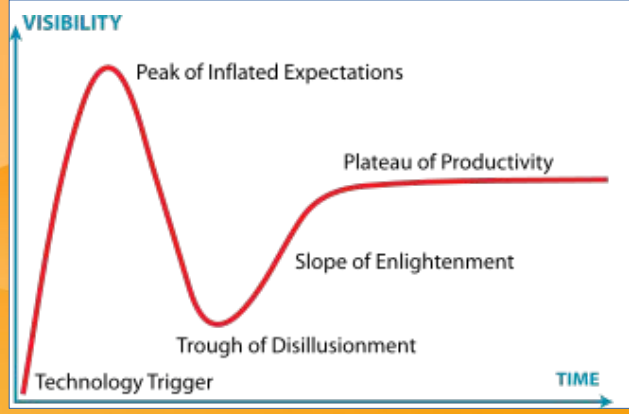
Doel presentatie

- Creëren awareness voor het cyber risico door IT standaardisatie
- Delen suggesties voor oplossingen

Indeling presentatie

- ICT trends
- Risicostapeling bij monoculturen
- Spreiden van het Malware risico

ICT trends



- Toename rekenkracht: meer gedigitaliseerde processen en gekoppelde systemen
- Gartner Hypecycle korter:
  testen onder druk, hergebruik (onveilige) componenten
- Outsourcing en schaalvergroting van ICT infrastructuren
- Slecht zicht op misbruik en reparatie kwetsbaarheden
- IT security is ‘n moeilijk vakgebied: kennis, tools, controverses
- Slechte ICT duurzaamheid = risico veiligheid BV NL
- Cybercriminaliteit floreert en professionaliseert:
  geringe pakkans, makkelijke opbrengst, asymmetrie, CAAS

Overal dezelfde ICT systemen biedt voordelen...

- ✓ Schaalvoordelen bij aanschaf software licenties
- ✓ Dezelfde hoge kwaliteit van ICT diensten
- ✓ Interoperabiliteit gegarandeerd (bestanden, macro's etc.)
- ✓ Standaardisatie van ICT kennis bij gebruik en beheer
- ✓ Plaats en Tijd onafhankelijk werken mogelijk

… Maar ook nadelen


vpro
npo
De huidige schermafdruk naar het klembord kopiëren
Zonder diversiteit is onze landbouw
niet levensvatbaar.

Een monocultuur is kwetsbaar

Vanuit efficiency benut de landbouw steeds minder soorten gewassen in grote monoculturen.

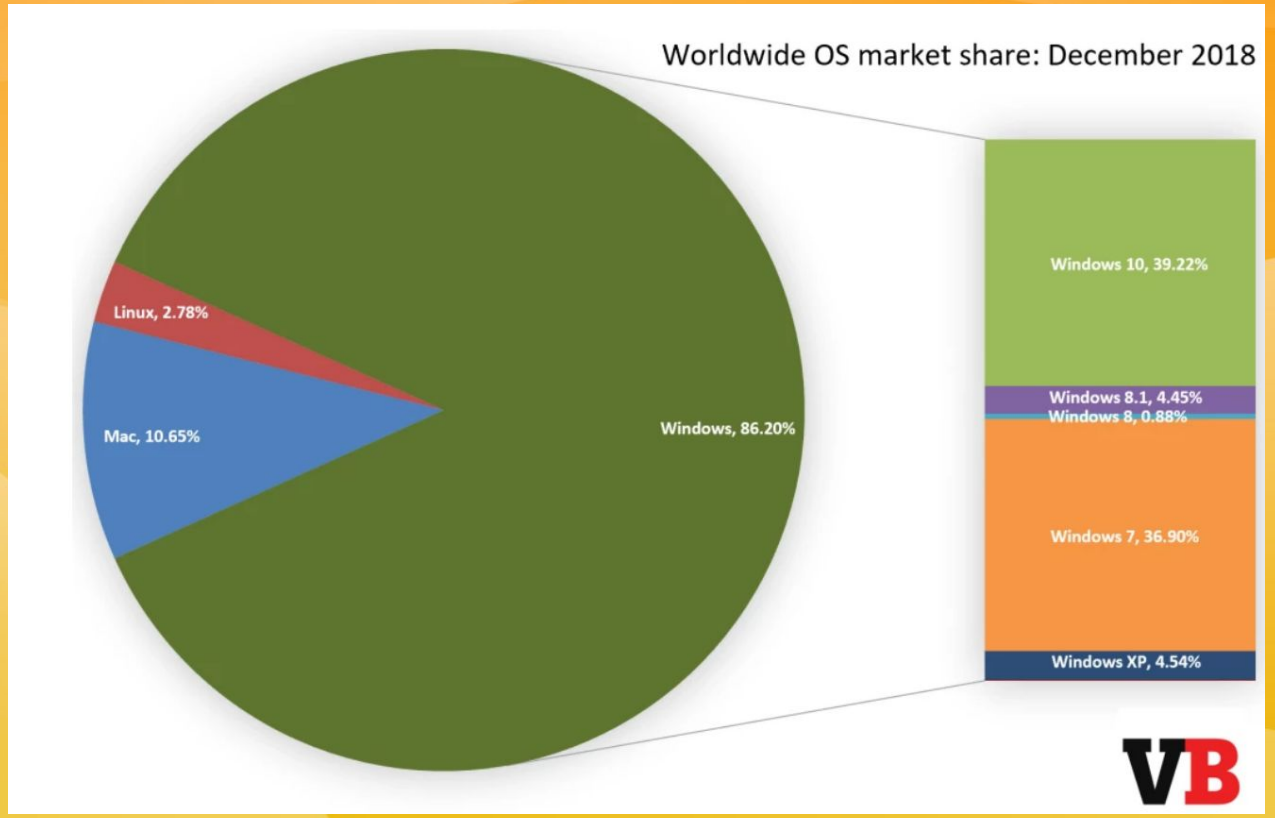
Traditionele gewassen worden steeds meer vervangen door uniforme soorten gewas met een hoge opbrengst per hectare.

Omdat de genetische basis versmalt, worden de oogsten steeds kwetsbaarder voor ziektes en plagen.

(World Resources Institute, 2001)

Software monoculturen op PC's

Meerdere voorbeelden: Operating Systems, Office suite, Adobe software



Bron: Netmarketshare.com

Epidemie kan in monocultuur makkelijker ontstaan

Besmettelijkheid ziekte

Disease	Basic reproduction number (R_0)	Critical Immunization threshold
Chickenpox	7 – 12	86-92%
Measles	11 – 18	91-94%
Mumps	7 – 14	86-93%
Pertussis	10 – 18	90-94%
Polio	5 – 7	80-86%
Rubella	6 – 12	83-92%
Smallpox	3 – 7	67-86%

R_0 values and critical immunization thresholds for common vaccine preventable diseases

Drempelwaarde voor epidemie

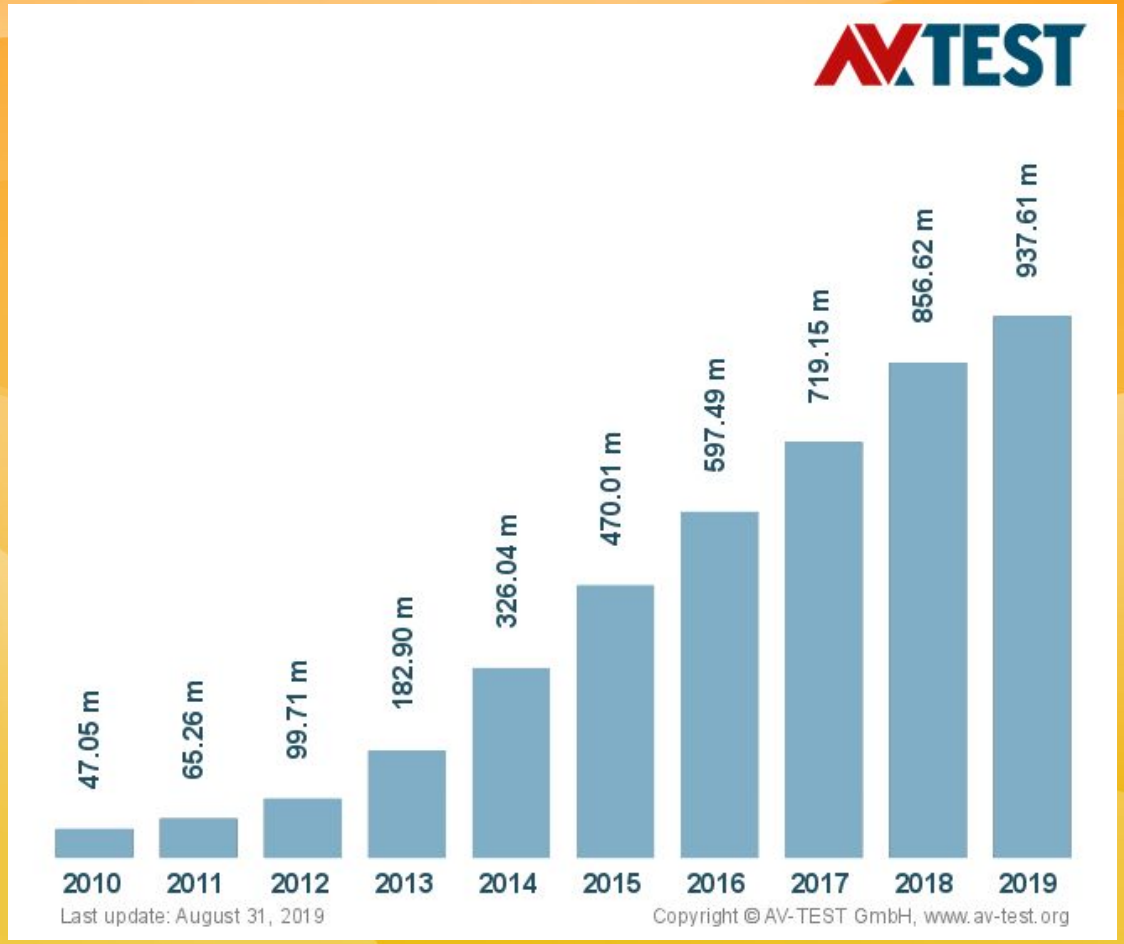
Software	Market Share	R_0
Linux	2,5	39,5
Mac OS X 10	6,0	16,6
Windows	91,5	1,1
Chrome	59,6	1,7
Internet Explorer	16,5	6,1
Firefox	12,3	8,1
MS Edge	5,7	17,7
Safari	3,7	27,3
Other	2,3	
Source:	*www.netmarketshare.com*	
Time frame:	*july 2017*	

Waarom geen conventie ‘ICT diversiteit’?

Pandemieën en plaagorganismen	Digitale verlamming
Conventie over biologische diversiteit	AFWEZIG
Invoerregels Douane	Open standaarden “pas toe of leg uit”
Beleid bevordering gezondheid planten en dieren; EU strategie gezondheidszorg	Beleid voor bescherming IT infrastructuur
EU beleid tegen overdracht ziektes tussen dier en mens	Wetten en beleid voor terugdringen cybercrime
WHO regels voor gezondheidszorg: monitoring en response	Beleid voor verminderen digitale verlamming, NL continuïteitsplan telco, beleid crisismanagement

Vergelijking enkele actieplannen in Project NL Nationale Veiligheid (2006)

Trend: steeds meer unieke malware



..ondertussen biedt Antivirus ook geen garantie

Virusscanner detecteren slechts 40%van de nieuwste virussen

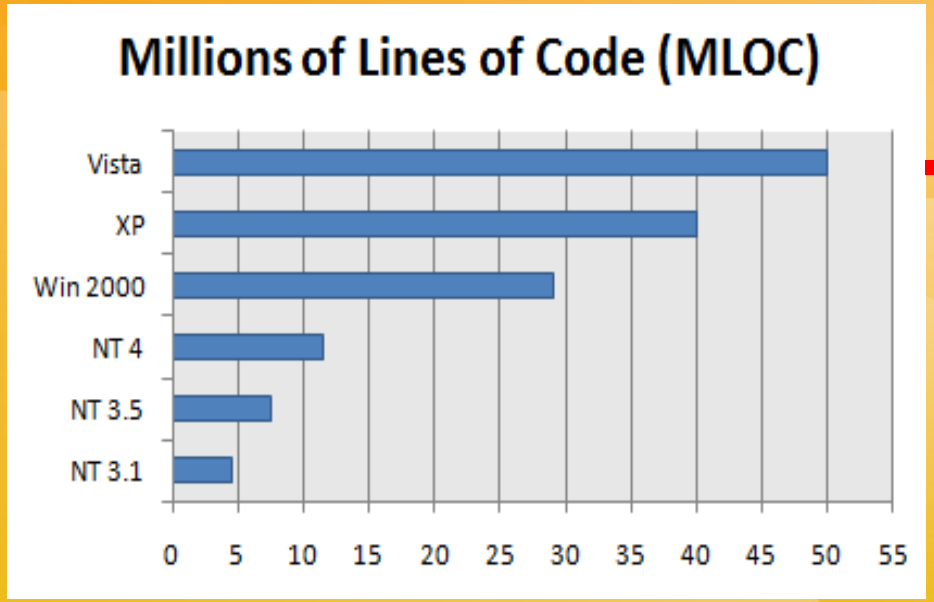
(FireEye Malware Intelligence Lab, Nov 2008)

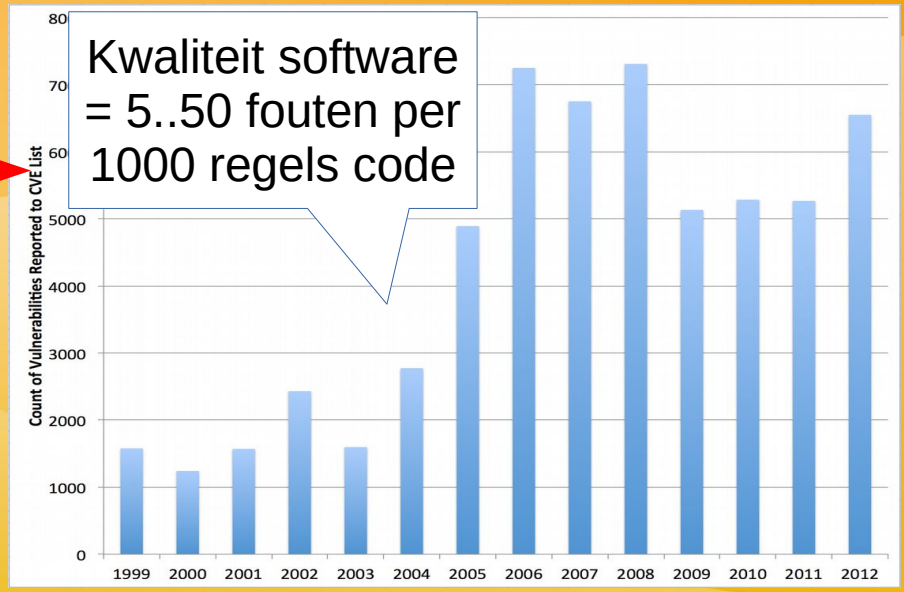
De meeste organisaties hebben **bijna 3 maanden nodig** voordat ze ontdekten dat hun systemen waren gecompromitteerd.

Mandiant M-trends 2019

In software kun je makkelijk inbreken

- Computers worden krachtiger (Wet van Moore)
- Software wordt steeds complexer
- **Meer complexiteit is kwetsbaarder**





21 % van de meest bezochte sites
draait software met bekende kwetsbaarheden (CSBN 2015)

Software updates kunnen lastig zijn

'When you buy a ship [of this size and complexity], you don't buy it today, you bought it twenty years ago. So what we put on the shelf and in the spec is probably what was good then.'

Mark Deller, commander air van het splinternieuwe Britse vliegdekschip HMS Queen Elizabeth, reageert op de zorgen die zijn geuit over de vele beeldschermen met Windows XP – dat al jaren niet meer wordt gëupdate door Microsoft – die in het schip te zien waren tijdens een openstelling voor het publiek. (The Guardian, 27 juni)

Technisch Weekblad 2017

Van incident naar cascade uitval

Als bezettingsgraad (p) perceel > 0,592746..
dan ontstaat een *“giant component”* (hier: p=0,6)

CSBN 2019:

Ontwrichting van de maatschappij ligt op de loer

Meer ICT diversiteit = hogere weerbaarheid

Analogie: 4 kleuren probleem

- Elke landkaart heeft max. 4 kleuren nodig om elk land een andere kleur te geven dan aangrenzende landen
- Computerbewijs uit 1976 in 2005 geverifieerd

- Analogie: ongelijke kleuren ↔ verspreiding malware stopt

Oplossing 1

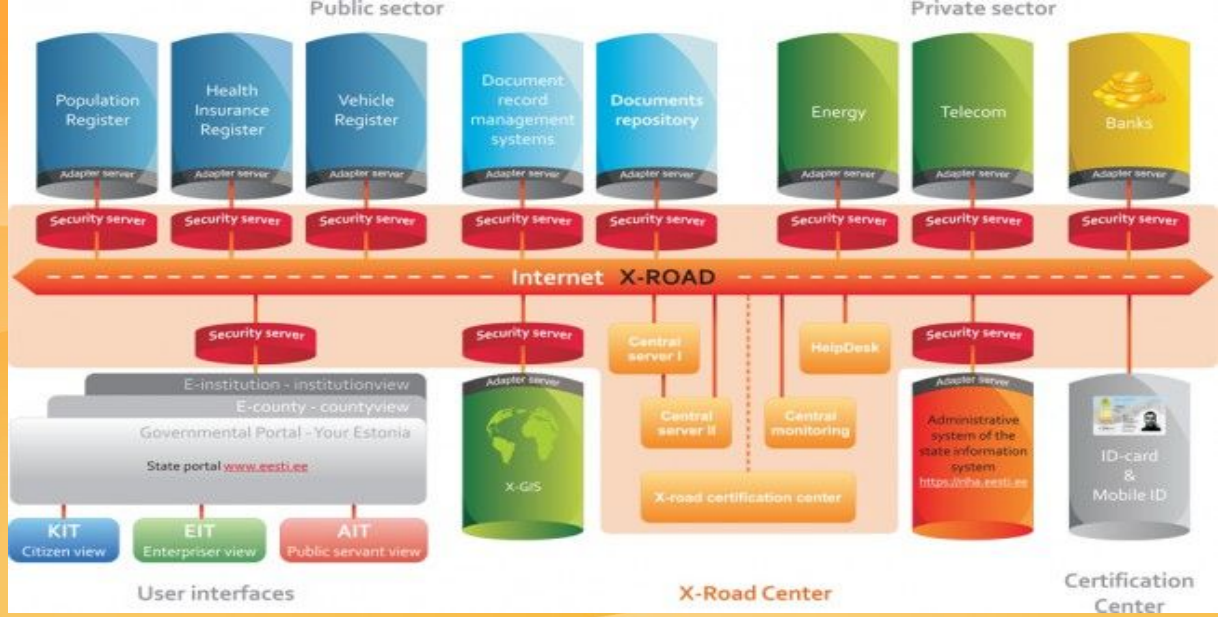
KNMI Meteo Sensor systeem @ Schiphol

- Uitval operationeel EN back-up systeem door fout in OS
- grote schade door vermindering capaciteit luchthaven

HET leerpunt: vermijd SPoF in Back-up systeem

- Andere hardware en infrastructuur,
- Ander Operating System,
- Andere programmeertaal,
- Andere dienstverlener

Oplossing 2: X-Road



- Estland 2007: 3 weken DDOS aanval van **alle online ICT-systemen**
- Daarna grote investeringen in beveiliging ICT + infra
- Estland **nu**: grote weerbaarheid tegen cyberaanvallen
- X-Road kenmerken:
  - Iedereen gebruikt eigen software op basis van Open Standaarden
  - Platform onafhankelijk

Samenvatting

- ICT is en blijft kwetsbaar, Cyber is dus een wapenwedloop
- Organisaties worden steeds meer ***afhankelijk van ICT***
- Cybercriminaliteit groeit en focust op grote aantallen
- Standaard software = ***single-point-of-failure*** voor malware;
  een Monocultuur **maximaliseert** het cyber risico
- *Murphy:* het is niet ***of*** dit gaat gebeuren, maar ***wanneer***
- Organisaties kunnen nog steeds standaardsoftware kiezen, maar …
  NL blijft kwetsbaar zolang bijna iedereen dezelfde software gebruikt

Korte termijn doelen

- Opstellen **Incident Escalatie Procedure**
- **Oefening** met handboek Datalek / ICT-crisis
- Netwerken logisch **compartimenteren**
- Aansluiten bij **Security Operation Center / CERT**
- **Verankeren IB** vanaf ontwerp t/m uitfaseren (BIA / PIA / PSA)
- Zorg voor voldoende **IB expertise**

Lange termijn doelen

- Breng afhankelijkheid van **monoculturen in beeld**
- Onderzoek waar en hoe **ICT-diversiteit** het Cyber Risico kan spreiden
- Toepassen **diversiteit in ontwerp** als architectuurprincipe voor gemeenschappelijke ICT-voorzieningen
- Check gebruik **Open Standaarden** tegen *vendor-lockin*
- Maak en check **afspraken over spreiding** in OS en software
  - met Leveranciers Management
  - met Software Lifecycle Management en vervanging **legacy**

Doel presentatie

- Creëren awareness voor het cyber risico door IT standaardisatie
- Delen suggesties voor oplossingen

Bedankt voor de aandacht!

Meer cyber publicaties op https://nl.linkedin.com/in/henkjanvdmolen

Waarom groeit *Cyber Crime* zo snel?

>> *Middel*

- CAAS: o.a. “one click” virus kits te koop
- Cyber crimineel is geen ICT expert meer
- Veel computers bevatten identieke software

>> *Motief*

- Steeds meer mensen en diensten online
- Alleen indirect contact met (anonieme) slachtoffers
- Verschillende verdienmodellen mogelijk
- Kleine kans op strafvervolging

>> *Gelegenheid*

- Technologie steeds complexer + kortere *Time to Market* = **meer onveilige systemen**
- Fouten in de beveiliging zijn moeilijk op te sporen
- Mogelijk doen cybercriminelen *Reverse Engineering* van patches
- Veel online systemen (IoT) worden slecht geüpdatet

Principes succesvolle cybercriminelen

- Zorg dat je niet wordt gepakt,
  gebruik multinationale aanvalspaden
- Start met de eenvoudigste aanval in het boekje
- *Stepping stone.* Kan je het doel niet rechtstreeks aanvallen, focus dan op kwetsbare koppelingen
- Vermijd gericht onderzoek, blijf beneden de pijngrens

www.isc.org/files/imce/IPv6-Cyber-Criminal-Opportunities-02.pdf

Enkele eerdere incidenten

Saudi Aramco Breach

In **August 2012**, malware partially wiped or totally destroyed the hard drives of **35,000 Aramco computers**. Saudi Aramco employees first noticed something was wrong on Aug. 15, as files disappeared and computers started to fail. A group calling itself the Cutting Sword of Justice claimed responsibility for the attack, which lasted just a few hours, citing the company's support of Saudi Arabia's royal family.

Friese gemeenten getroffen door ransomware – 10 juni 2015

Drie Friese gemeenten zijn deze week getroffen door ransomware. Ongeveer zeshonderd medewerkers van de gemeenten Ooststellingwerf, Weststellingwerf en Opsterland moesten hun werk hierdoor enkele uren onderbreken. De gemeenten zijn inmiddels weer bereikbaar.

9 aug 2012 Dorifel-virus: meer dan 30 instellingen besmet

Het Dorifel-virus duikt bij **diverse gemeenten** op en besmet bestanden. Burgerdiensten kunnen niet meer geleverd worden en medewerkers kunnen niet meer mailen. Paspoorten kunnen bijvoorbeeld niet meer opgehaald worden. Het computervirus heeft inmiddels meer dan dertig instellingen en zo'n **3000 computers besmet**. Vooral gemeenten zijn getroffen, maar volgens het Nationaal Cyber Security Centrum (NCSC) hebben ook universiteiten en bedrijven er last van.

Het virus is een zogeheten Trojaans Paard dat ongemerkt via e-mail systemen binnen dringt en zo netwerken besmet. Onbevoegden kunnen makkelijk meekijken in de computer, terwijl de gebruiker zelf niets merkt. Het virus wordt gevoed door een botnet: een netwerk van computers die allemaal besmet zijn met kwaadaardige software en dat zichzelf steeds update. Hierdoor wordt het virus constant sterker.

Meest aangevallen software

Windows

Adobe Acrobat

Recorded Future: ‘Soft Target:
Top 10 Vulnerabilities Used by Cybercriminals’-CTA-2018-0327

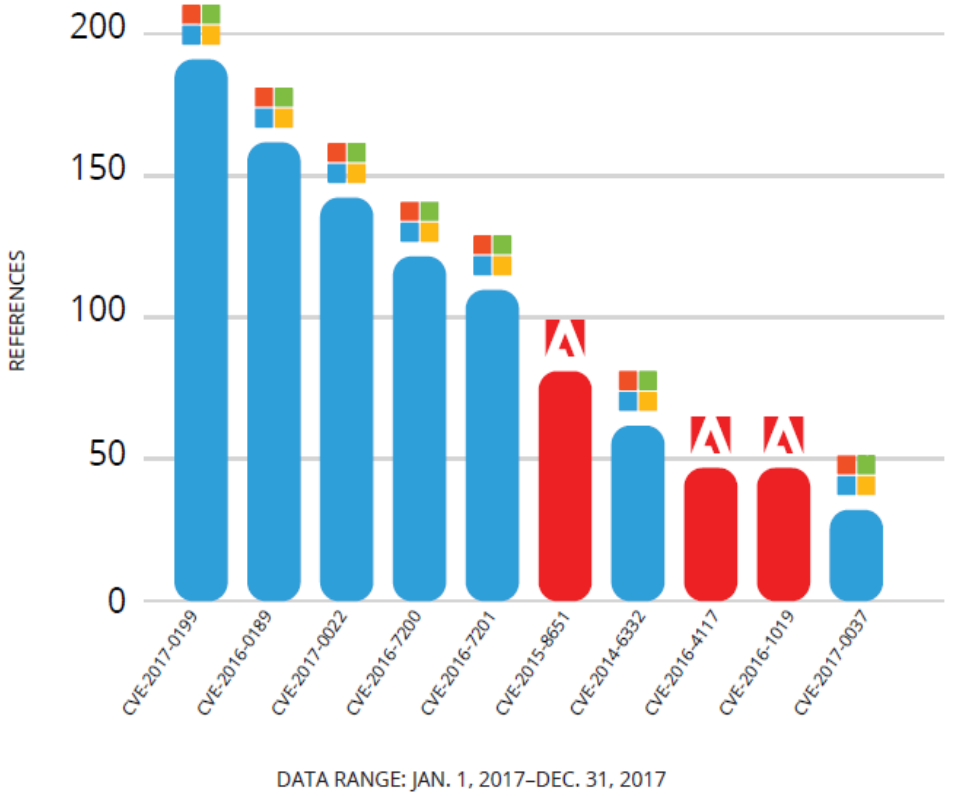
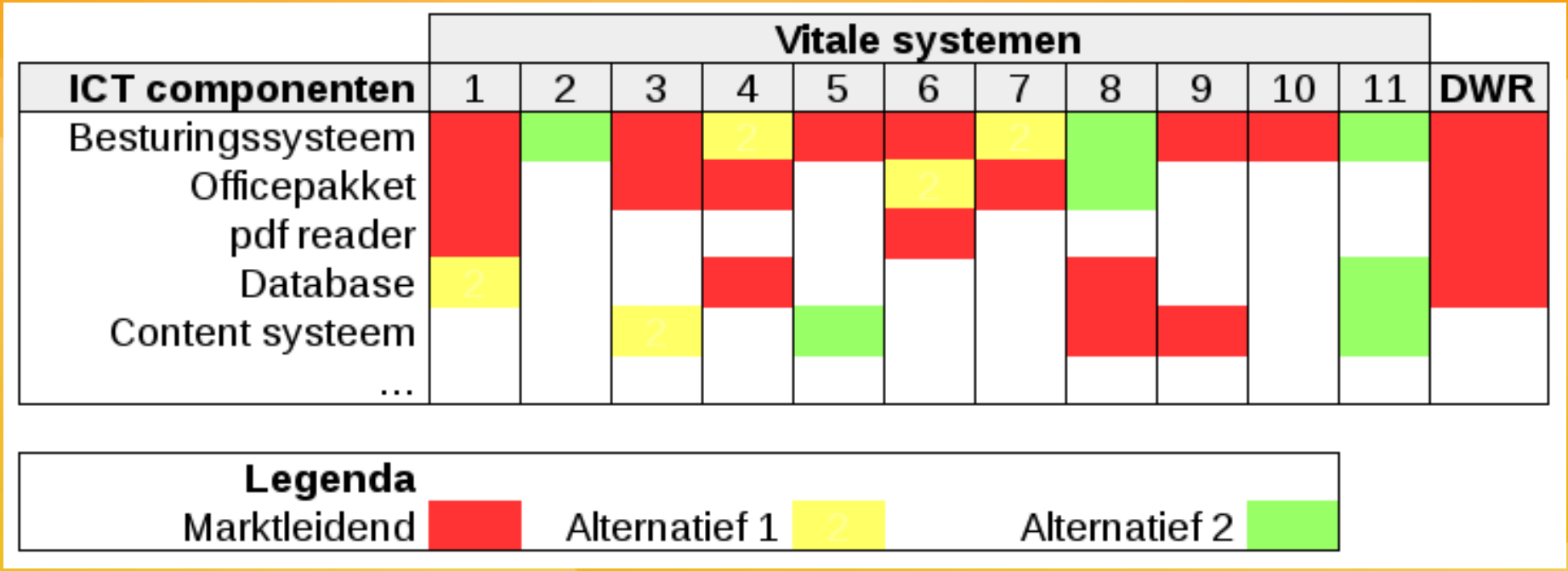


Image 1: References to vulnerability exploitation by exploit kits or phishing.

Voorbeeld *Cyber Heat Map*

Onderzoek voor welke systemen ICT diversiteit bestaat



Beveiliging wordt minder effectief
Cyber is een wedloop

Beveiliging tegen malware	Acties Cybercriminelen
Besmettingskans verlagen door preventie: • SIEM, Intrusion Prevention System, firewall; • AV-software (on access scan) met patroonherkenning; • legale, white list software; • beperkte gebruikersrechten, hardening; • software compartimenten; • goede procedures voor changes / updates; • vergroten kennis, bewustzijn; • preventieve security audits.	***Verhogen besmettingskans malware:*** • meerdere aanvalspatronen in malware; • aanval combineren met social engineering; • delen van kennis en malwarecode; • testen malware, o.a. met antivirussoftware; • 'fuzz' testen software op kwetsbaarheden; • website levert malware op maat; • massaal en snel malware verspreiden; • encryptie, code obfuscation in malware; • gerichte malware ('precision ammo').
Verbeter ontsmetting (detectie, correctie): • meerdere AV-software (voor geplande scans); • SIEM, Intrusion Detection System, logging; • Management procedures voor incidenten en changes, incl. Incident Response Plan; • vergroten kennis, bewustzijn, follow-up security audits.	***Verlagen uitval besmette computers:*** • rootkits, stealth malware, data encryptie; • malware sneller updaten dan antivirussoftware; • imitatiegedrag legitieme software; • ***Business Continuity Plans*** • malware activeert zichzelf bij bepaalde condities; • patchen van besmette computers (!)

Het internet als malware biotoop

Analogie: verspreiding ziektekiemen

- SIS model *(Susceptible – Infected – Susceptible)*
- 2 Parameters:
  - β = Kans op overdragen infectie per contact
  - γ = Kans op “genezing”
- Met β, γ is uit te rekenen:
  - Epidemie Ja / Nee
  - Max % populatie besmet

Diversiteit vergt gebruik van Open Standaarden

"As a matter of logic alone...

If you care about the security of the commonwealth, then you care about:

- the risk of a computing **mono-culture**,
- **barriers** to diversification,
- user-level **lock-in** and
- breaking the proprietary format stranglehold on the commonwealth.

Until that is done,
the mono-culture **bomb** keeps ticking"
(Daniel Geer: Massachusetts assaults monoculture)

Dealing with the lack of diversity

The IT industry has tended towards dominant suppliers. As systems become increasingly interconnected, a common vulnerability could trigger **cascading failures**. Diversity can be a security issue as well as a competitive one.

Options to promote logical diversity

1. Promoting **open standards** to facilitate market entry
2. **Promoting diversity** in the procurement process and e-Government
3. Advise competition authorities when lack of diversity presents a **security issue**

(Enisa, 2008)