



ENJOY SAFER TECHNOLOGY™

Een niet zo'n coole presentatie over cybersecurity.

Dave Maasland
Managing Director
ESET Nederland



Dave@eset.nl







CRUNCH NETWORK

Why Breach Detection Is Your New Must-Have, Cyber Security Tool

BANEN

Nieuws Cultuur & Leven

Economie

Cursisten leren bij PwC hoe zij om moeten gaan met een te loodsen. © Raymond Rutting/de Volkskrant

Bedrijven zijn zo le

There are two types of companies: those who have been hacked, and those who don't yet know they have been hacked.

John Chambers
Chief Executive Officer of Cisco

n pakken, lukt



ENJOY SAFER TECHNOLOGY™

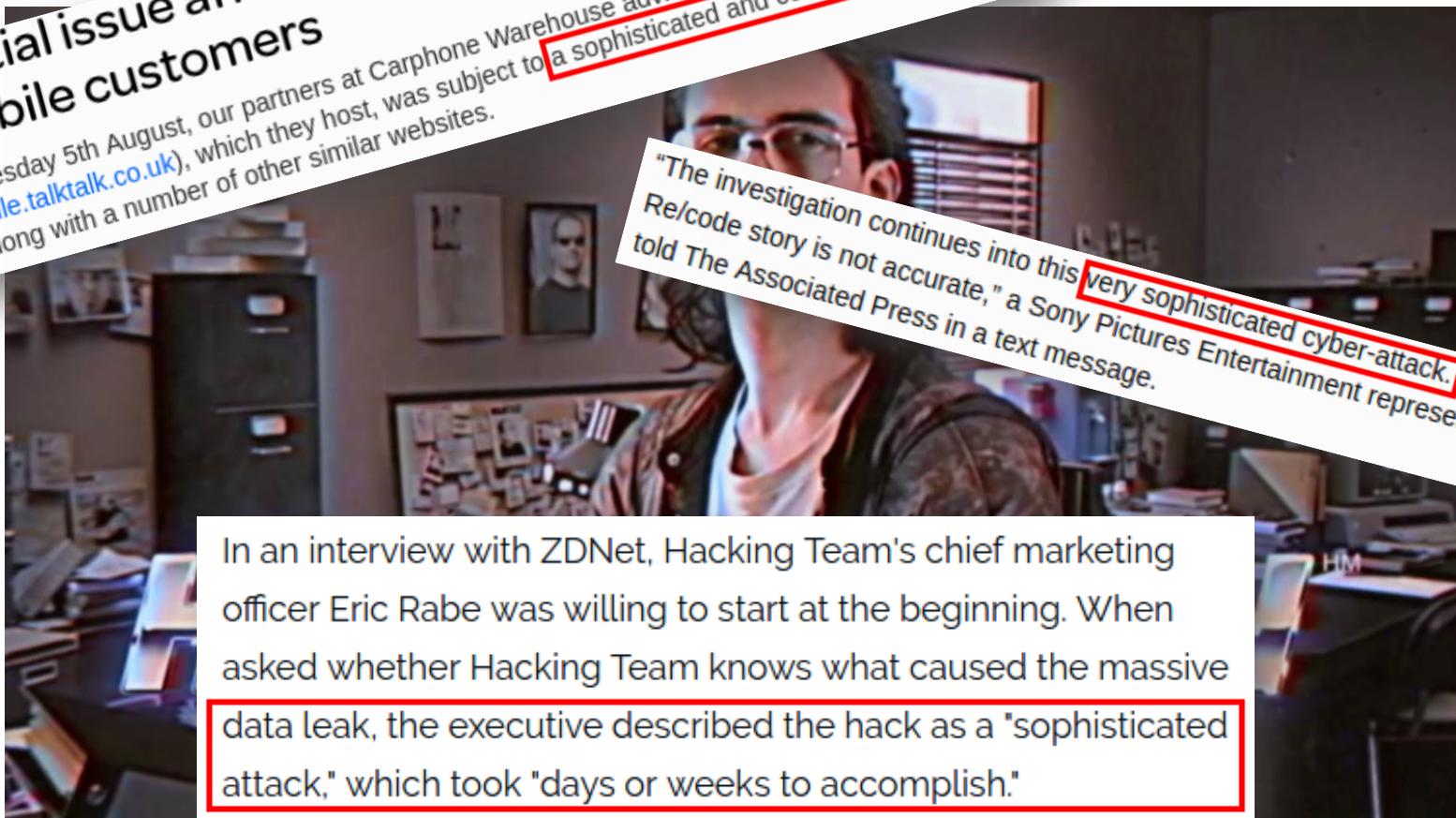


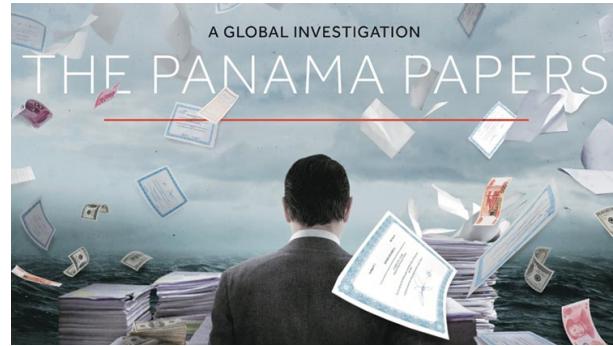
De w derd

Potential issue affecting the personal information of mobile customers

On Wednesday 5th August, our partners at Carphone Warehouse advised us that our mobile sales site (mobile.talktalk.co.uk), which they host, was subject to a sophisticated and co-ordinated cyber attack, along with a number of other similar websites.

"The investigation continues into this very sophisticated cyber-attack. The Re/code story is not accurate," a Sony Pictures Entertainment representative told The Associated Press in a text message.





The hackers from Impact Team told Motherboard: “*We worked hard to make fully undetectable attack, then got in and found nothing to bypass....Nobody was watching. No security. Only thing was segmented network. You could use Pass1234 from the internet to VPN to root on all servers.*”



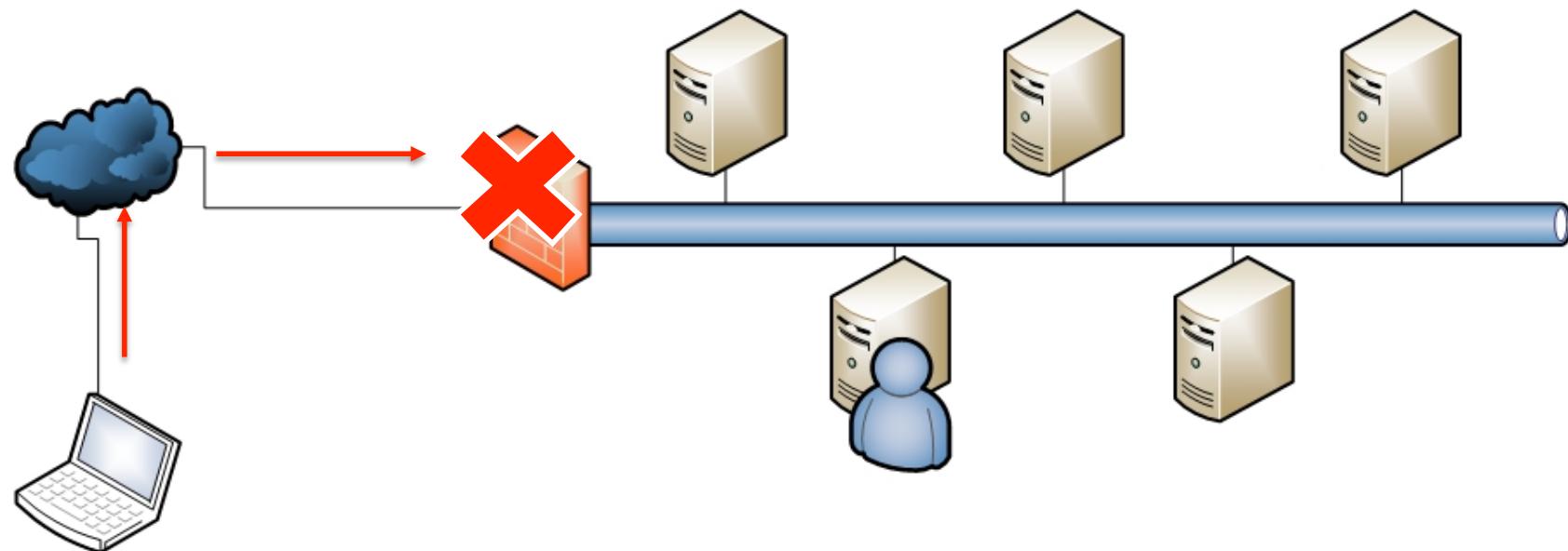
ENJOY SAFER TECHNOLOGY™



ENJOY SAFER TECHNOLOGY™

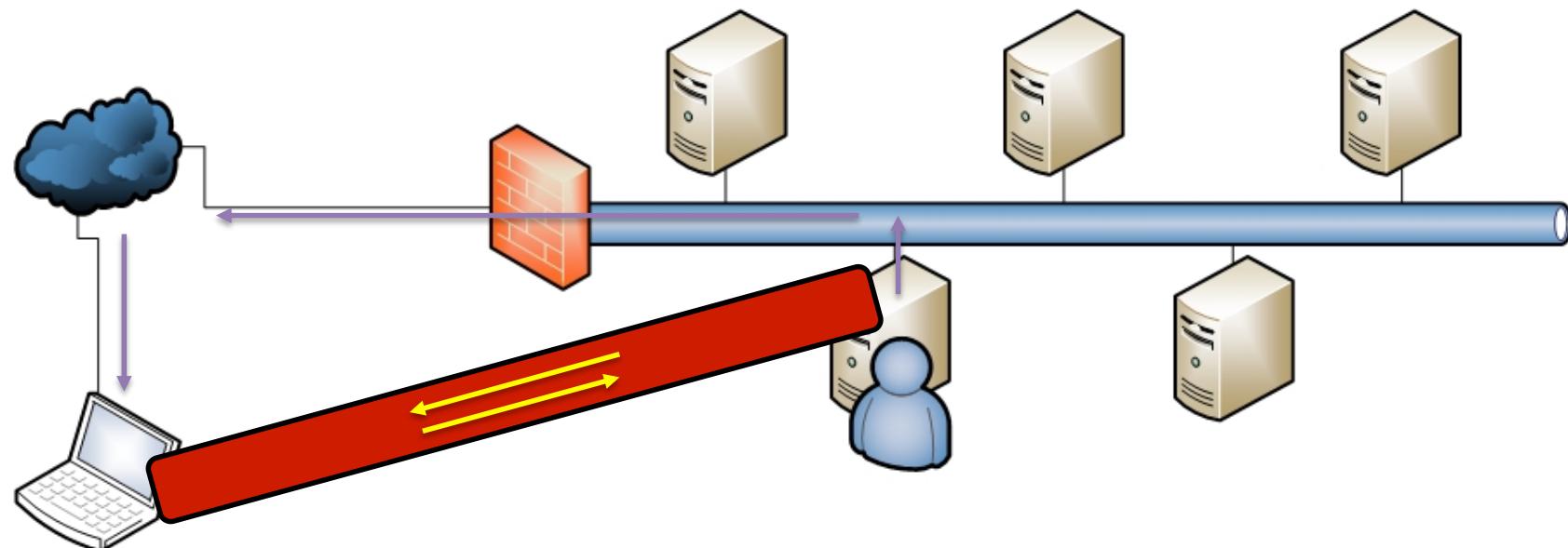


De super-geavanceerde-cyber-aanval:



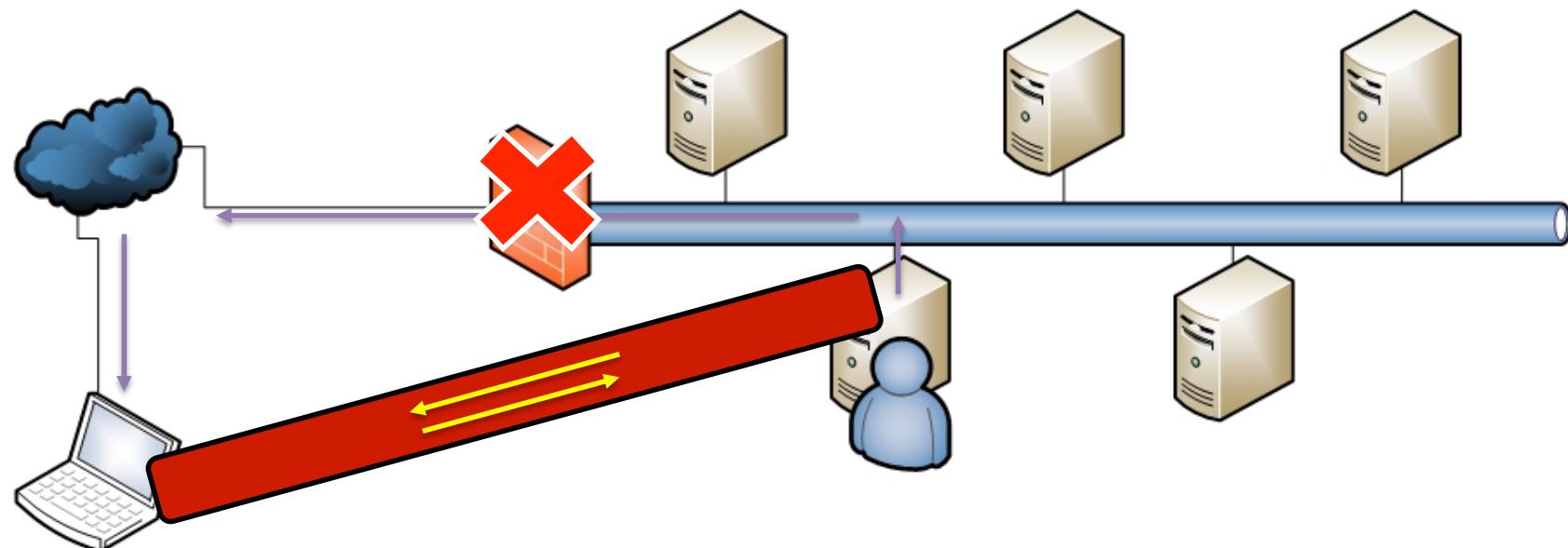


De super-geavanceerde-cyber-aanval:





Het internet is magisch:





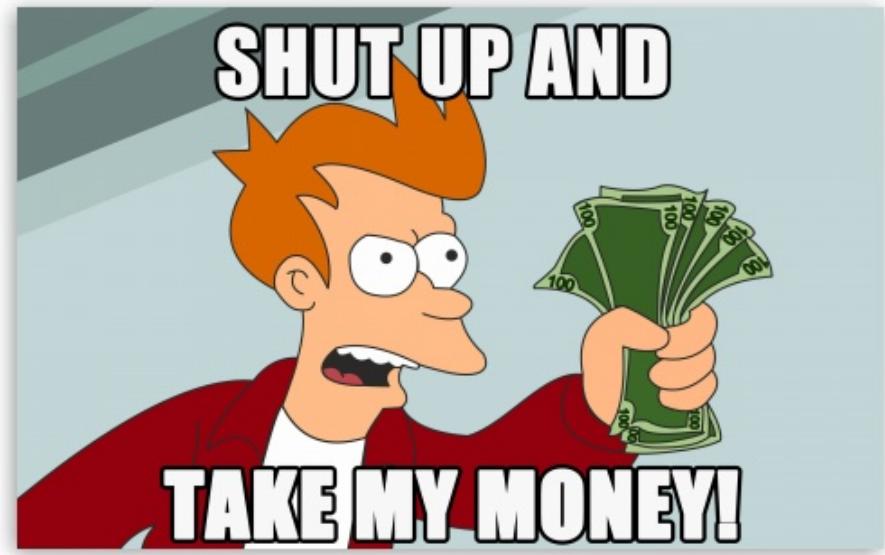
De super-geavanceerde-cyber-aanval:

The screenshot shows an email message in Microsoft Outlook. The subject is "Accountverificatie - Message (HTML)". The recipient is "Donny Maasland | ESET Nederland". The message body starts with "Beste Donny," followed by a paragraph about account verification due to the Data Protection Act. It instructs the user to log in using their Windows account at the URL <https://████████.nl/verify/>. The message ends with "Na het inloggen is geen verdere actie vereist, alvast bedankt voor jullie medewerking, Afdeling ICT █████".

The image displays two screenshots of the Microsoft Account Verification page. The top screenshot shows the login interface with fields for "User name" and "Password", and a "Sign in" button. The bottom screenshot shows the success message "Thank you, your account has been verified." Both screenshots mention "Connected to Microsoft Exchange" and "© 2010 Microsoft Corporation. All rights reserved."



ENJOY SAFER TECHNOLOGY™





The cool kids table





It works:



ENJOY SAFER TECHNOLOGY™



PREVENTIE

**voorkomen is
stuk effectiever**



ENJOY SAFER TECHNOLOGY™



WAT WETEN WE OVER DATALEKKEN:

1. IN 69% VAN ALLE GEVALLEN WORDT MALWARE GEBRUIKT.
2. IN 80% VAN ALLE GEVALLEN WORDT HACKING* GEBRUIKT.
(MALWARE EN HACKING SAMEN IN 61% VAN DE GEVALLEN)
3. IN 97% VAN ALLE GEVALLEN VEROUDERDER SOFTWARE, NON-HARDENED INSTELLINGEN EN ZWAKKE WACHTWOORDEN.

In 80% van alle hacks zijn paswoorden: default, niet aanwezig, gestolen, geraden of kraakbaar.

Ponemon breach report 2015



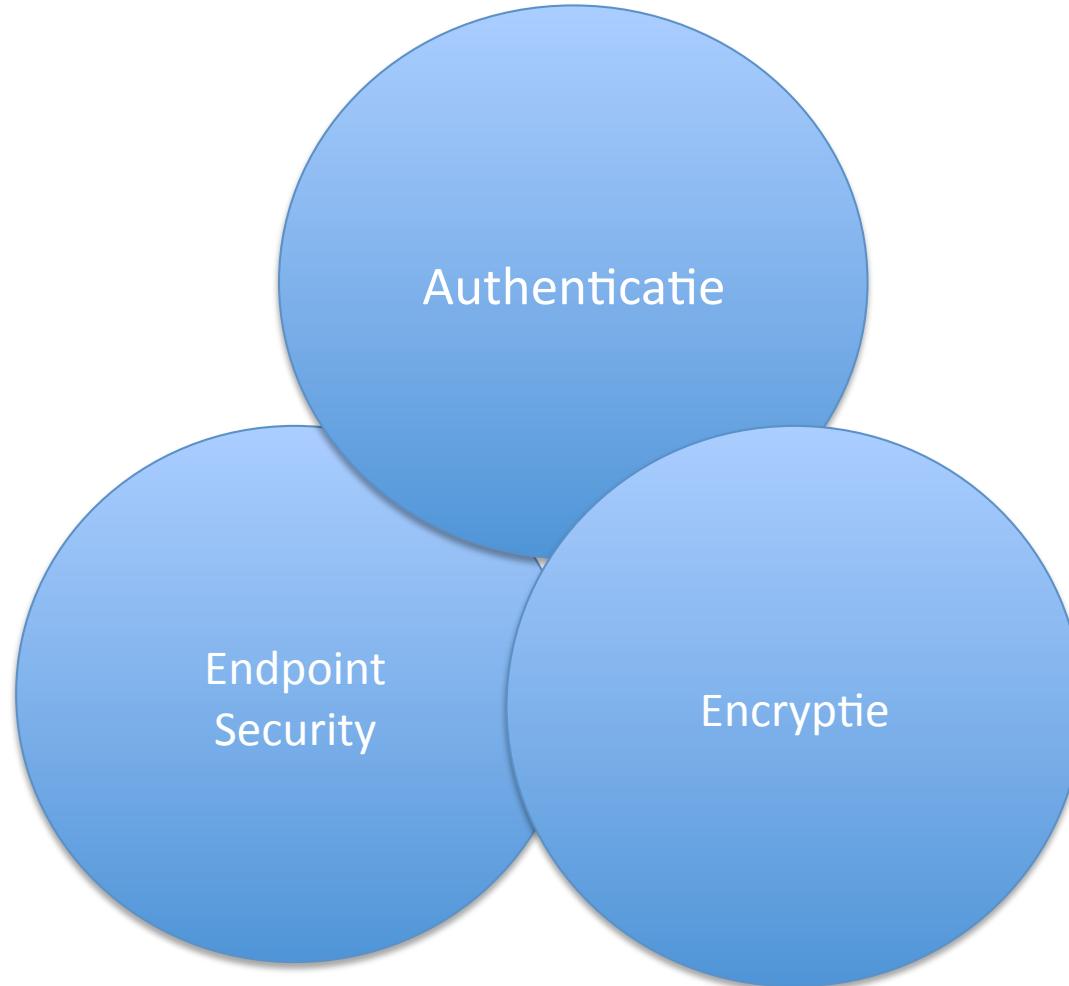
ENJOY SAFER TECHNOLOGY™



ENJOY SAFER TECHNOLOGY™



Focus:



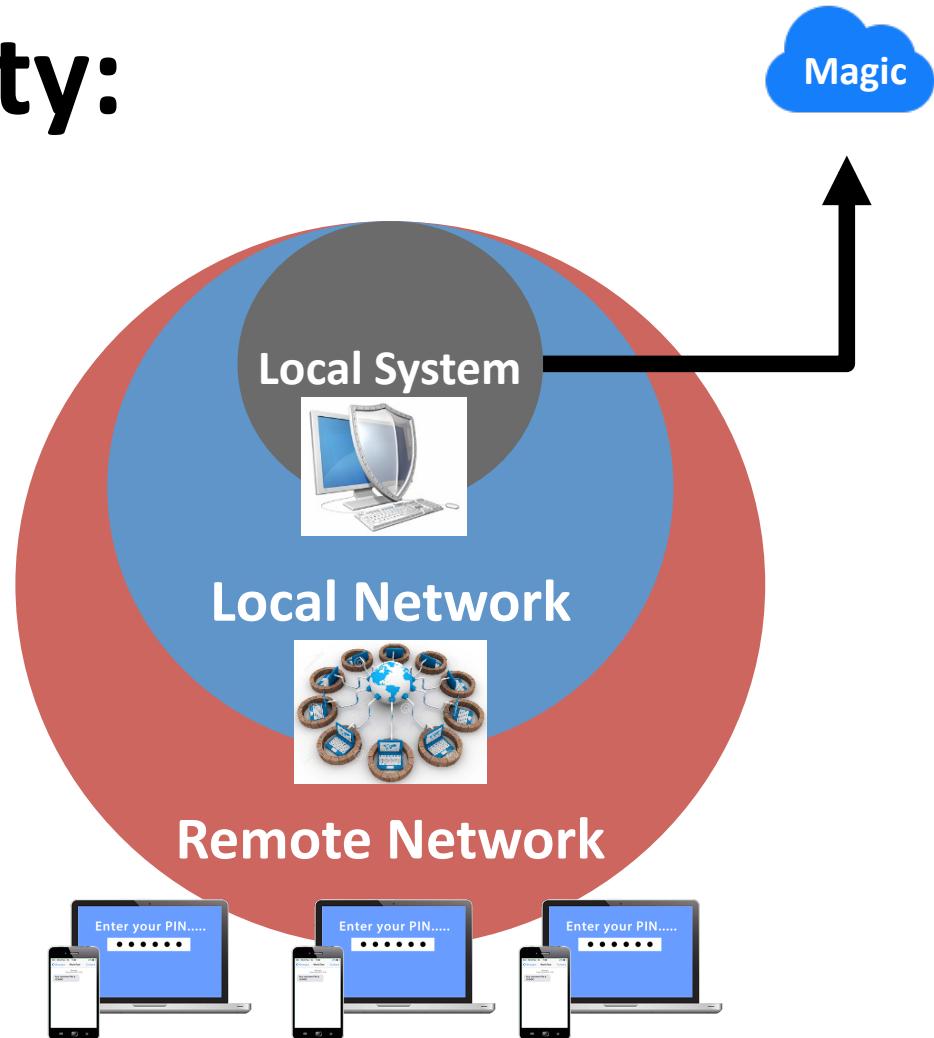


Gelaagde Security:

- Endpoint Security
- Mobile Security
- Encryptie

- DLP
- Server Security

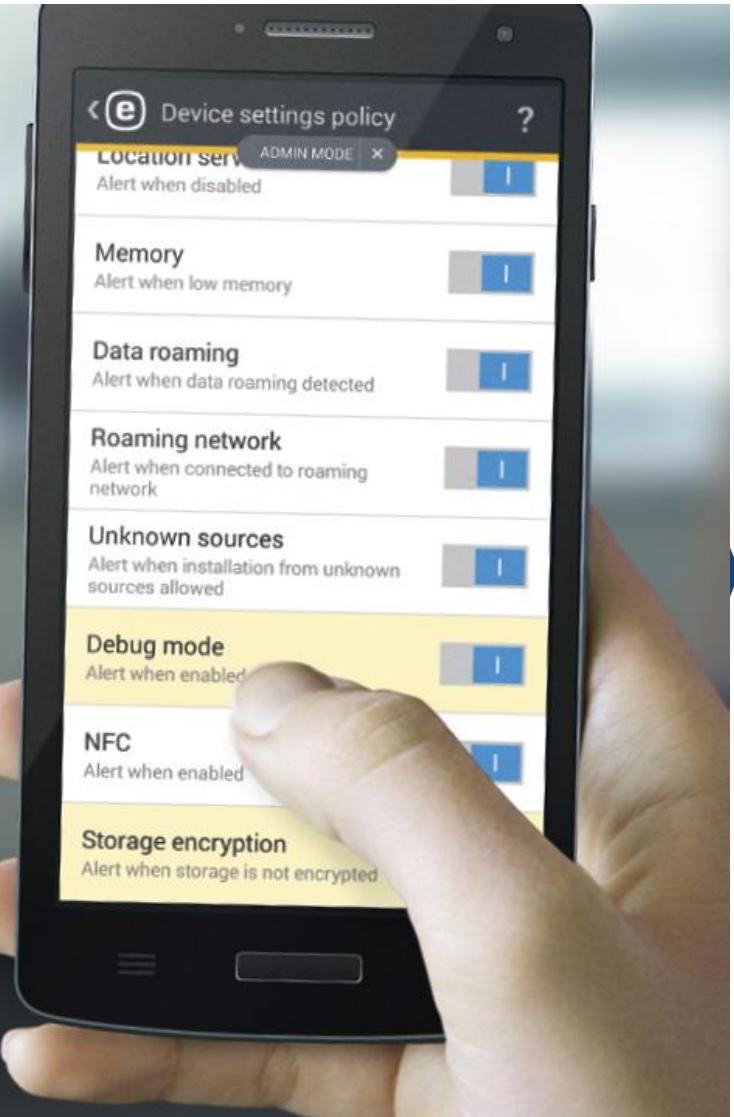
- Authenticatie
- Patch Management





MONITOR PRE-DEFINED DEVICE SETTINGS
FOR COMPLIANCE

eset® ENDPOINT SECURITY
FOR ANDROID





Antispam:

The screenshot shows the ESET Remote Administrator interface under the 'Edit Policy - Settings' tab. In the left sidebar, 'Antispam protection' is selected under the 'SERVER' section. The main window displays the 'Rules' configuration for 'MAILBOX DATABASE PROTECTION'. A modal window titled 'Rules' lists several rules with checkboxes:

Active	Name	Level	Hits
<input type="checkbox"/>	Dangerous system file attachments	Attachment processing	0
<input checked="" type="checkbox"/>	Dangerous executable file attachments	Attachment processing	0
<input type="checkbox"/>	Forbidden archive file attachments	Attachment processing	0
<input checked="" type="checkbox"/>	Common ransomware droppers	Attachment processing	0
<input type="checkbox"/>	Password protected archive file attachments	Result processing	0

A callout box highlights the 'Dangerous executable file attachments' rule, which is checked. Another callout box shows a list of checked executable file types:

- Executable files
 - Windows Executable (*.exe; *.dll; *.sys; *.drv; *.ocx; *.scr)
 - MS-DOS Executable (*.exe)
 - ELF Executable and Linkable format (e.g. Linux) (*.elf)
 - Adobe Flash (*.swf)
 - Java Class Bytecode (*.class)
 - Windows Installer Package (*.msi)
 - Apple OS X Universal binary executable
 - Apple OS X Mach-O binary executable
 - Android executable (*.dex)

Below this, another callout box lists common ransomware dropper extensions:

- *.js
- *.hta
- *.docm
- *.xlsm
- *.pptm
- *.vbs
- *.bat

A final callout box provides a note about Microsoft Office files:

* In this case **Microsoft Office files with Macro's will also be blocked (docm, xlsm and pptm)**. When such files are used within your organization, this rule has to be adjusted or disabled.



Firewall:

Firewall rules

Rules define how the Personal firewall handles incoming and outgoing network connections. Rules are evaluated from top to bottom, action of first matching rule is applied.

Name	Enabled	Protocol	Profile	Action	Direction	Local	Remote	Application
Deny network connections for wscript.exe (native)	<input checked="" type="checkbox"/>	Any	Any profile	Deny	Both			C:\Windows\System32\wscript.exe
Deny network connections for wscript.exe (SysWOW64)	<input checked="" type="checkbox"/>	Any	Any profile	Deny	Both			C:\Windows\SysWOW64\wscript.exe
Deny network connections for cscript.exe (native)	<input checked="" type="checkbox"/>	Any	Any profile	Deny	Both			C:\Windows\System32\cscript.exe
Deny network connections for cscript.exe (SysWOW64)	<input checked="" type="checkbox"/>	Any	Any profile	Deny	Both			C:\Windows\SysWOW64\cscript.exe
Deny network connections for powershell.exe (native)	<input checked="" type="checkbox"/>	Any	Any profile	Deny	Both			C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
Deny network connections for powershell.exe (SysWOW64)	<input checked="" type="checkbox"/>	Any	Any profile	Deny	Both			C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Deny network connections for ntvdm.exe	<input checked="" type="checkbox"/>	Any	Any profile	Deny	Both			C:\Windows\System32\ntvdm.exe

Add Edit Remove

Show built in (predefined) rules

OK Cancel

Application

- C:\Windows\System32\wscript.exe
- C:\Windows\SysWOW64\wscript.exe
- C:\Windows\System32\cscript.exe
- C:\Windows\SysWOW64\cscript.exe
- C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
- C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
- C:\Windows\System32\ntvdm.exe

IMPORTANT

- This policy only works in combination with ESET Endpoint Security because of the integrated firewall module.
- For these rules it also applies that legitimate applications can use the executables. We therefore recommend you to test this before fully implementing the policy within your organization.



ENJOY SAFER TECHNOLOGY™



HIPS:

The screenshot shows the 'Edit Policy - Settings' window for ESET NOD32 Antivirus. In the center, the 'HIPS rules' section displays a table of rules. The table has columns: Rule, Enabled, Action, Sources, Targets, and Location. There are four rules listed:

Rule	Enabled	Action	Sources	Targets	Location
Deny child processes from dangerous executables	<input checked="" type="checkbox"/>	Block	Applications	<input checked="" type="checkbox"/>	
Deny script processes started by explorer	<input checked="" type="checkbox"/>	Block	Applications	<input checked="" type="checkbox"/>	
Deny dangerous child processes from Office 2013 processes	<input checked="" type="checkbox"/>	Block	Applications	<input checked="" type="checkbox"/>	
Deny dangerous child processes from Office 2016 processes	<input checked="" type="checkbox"/>	Block	Applications	<input checked="" type="checkbox"/>	

A callout box labeled 'IMPORTANT' contains the following note:

- These rules block executables that may also be used by legitimate applications. We therefore recommend you to test this before fully implementing the policy within your organization.

Three detailed views of the 'Location' column are shown in callout boxes:

- Deny child process from dangerous executables.** Shows a list of executables: C:\Windows\System32\wscript.exe, C:\Windows\SysWOW64\wscript.exe, C:\Windows\System32\cscript.exe, C:\Windows\SysWOW64\cscript.exe, C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe, C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe, and C:\Windows\System32\ntvdm.exe.
- Deny script processes started by explorer** Shows a list of executables: C:\Windows\System32\wscript.exe, C:\Windows\SysWOW64\wscript.exe, C:\Windows\System32\cscript.exe, and C:\Windows\SysWOW64\cscript.exe.
- Deny Dangerous child processes from Office 201x** Shows a list of executables: C:\Windows\System32\cmd.exe, C:\Windows\SysWOW64\cmd.exe, C:\Windows\System32\wscript.exe, C:\Windows\SysWOW64\wscript.exe, C:\Windows\System32\cscript.exe, C:\Windows\SysWOW64\cscript.exe, C:\Windows\System32\ntvdm.exe, C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe, and C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.

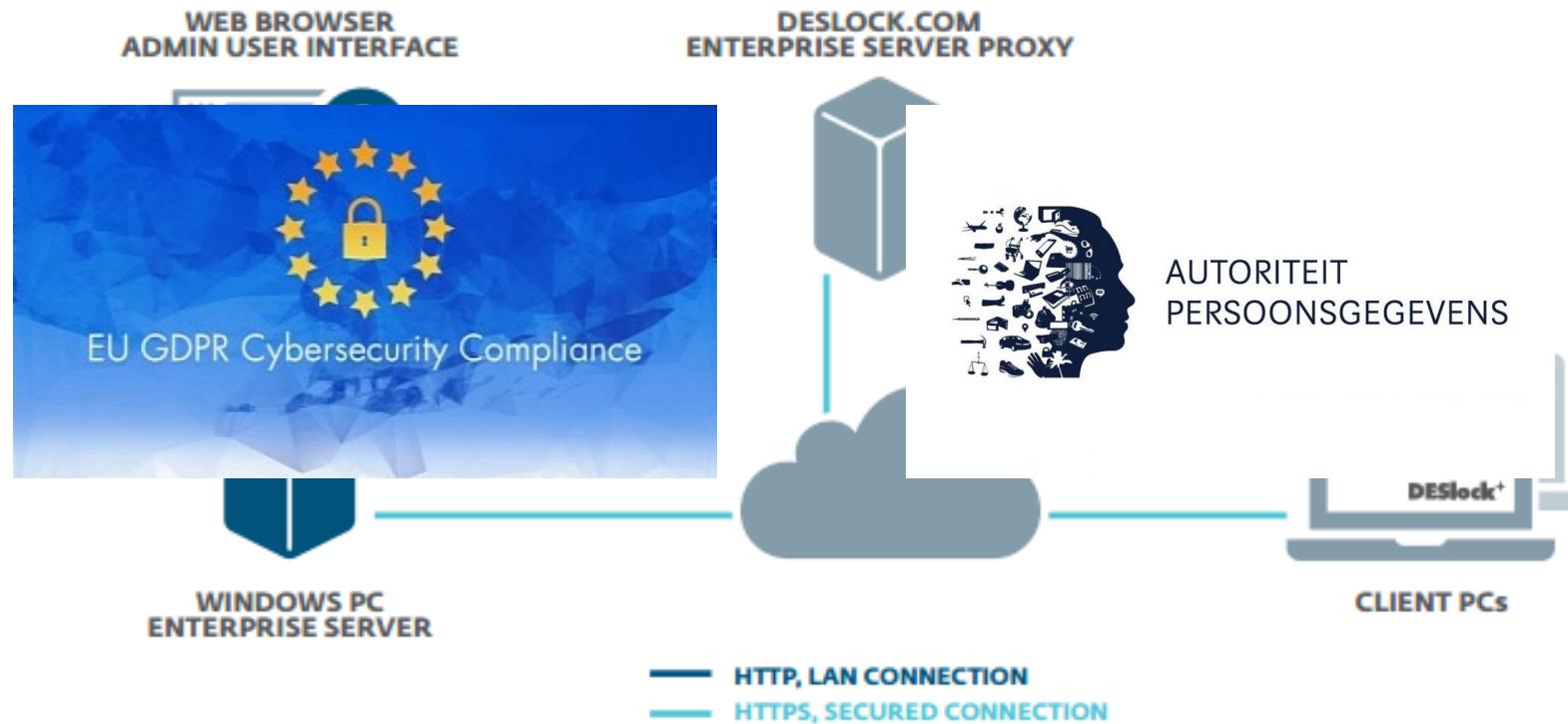


2-Factor Authentication





Encryption





De uitdaging:





The proposition



ESA	Safetica
2FA	Data Loss Prevention

--	--





Managed:

Managed Services Level

Assessment



Weerbaar



Core products

EP Protection



Mobile/Tablet Protection



Compliant



DESLock

Data
Encryption



ESA

2FA



MaaS360
by Fiserv, an IBM company

Safetica

Data Loss
Prevention



ENJOY SAFER TECHNOLOGY™



ENJOY SAFER TECHNOLOGY™



ENJOY SAFER TECHNOLOGY™

Thank You

www.WeLiveSecurity.com

Dave@eset.nl