

Securing the Future of IT

The Digital Transformation and its Impact

Version 1.0 | June 2016



A Journey Into The Present

Digital transformation of businesses and the world

Implications on the protection of infrastructures

- Securing The Cloud
- Securing The Things
- Digital Transformation of Crime
- Securing against Advanced Threats

Cloud

Things

Crime

Threats



Digital Transformation

In 2016?



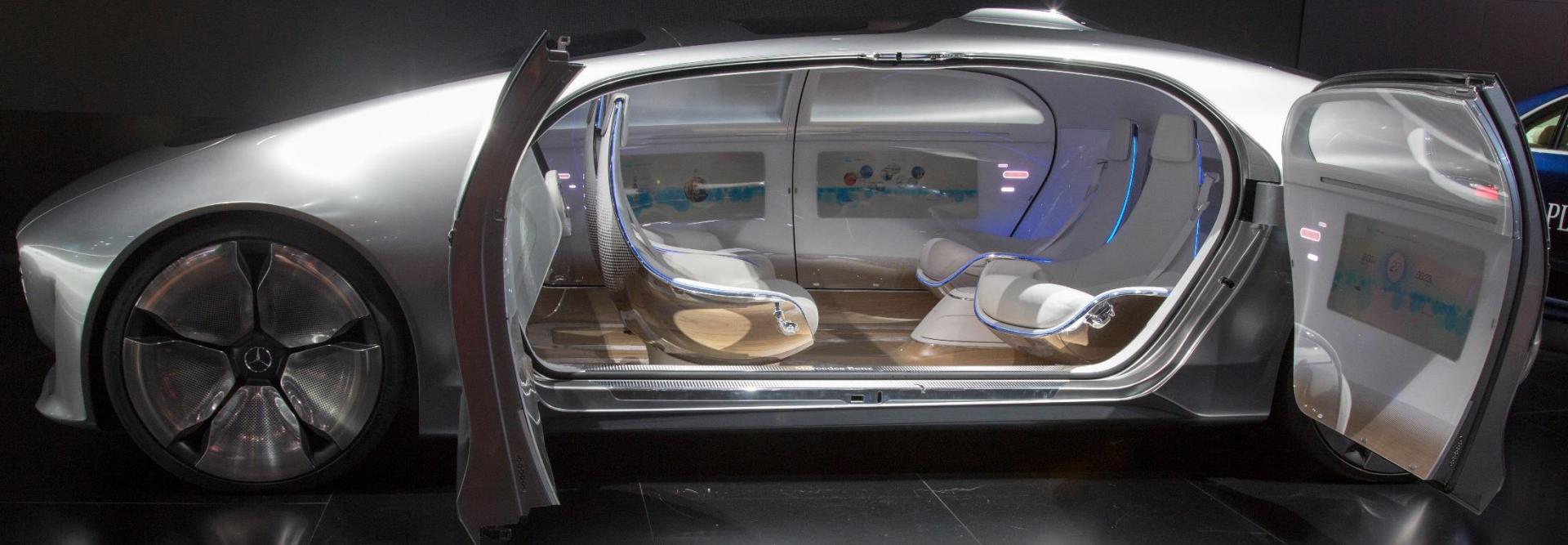
Smart Cities



Smart Cities



Digital Transformation



Digital Transformation



Digital Transformation

SUPERMARKETS...



Digital Transformation

Thesis 1

IT will move into the
CEO's responsibility away
from the CFO



Digital Transformation

Consequences for IT infrastructure

- Location of users, data, and applications do not matter anymore
- Everyone and everything will be everywhere and permanently moving



Digital Transformation

Thesis 2

Stability of location will disappear for IT security.
Security must be everywhere, just like IT components.



Digital Transformation – Essence

Where is the Firewall!

Digital Transformation – Essence

WTF!



Implications on Infrastructure Protection

Cloud

Things

Crime

Threats



Implications on Infrastructure Protection

Cloud

Things

Crime

Threats



Why Cloud At All?

So much more flexible,
elastic, and agile



Challenge

Will cloud-based
infrastructures ever be
as secure as on-premises ones?



Cloud

Thesis 3

Cloud-based
infrastructures can be
MORE secure than
on-premises ones!



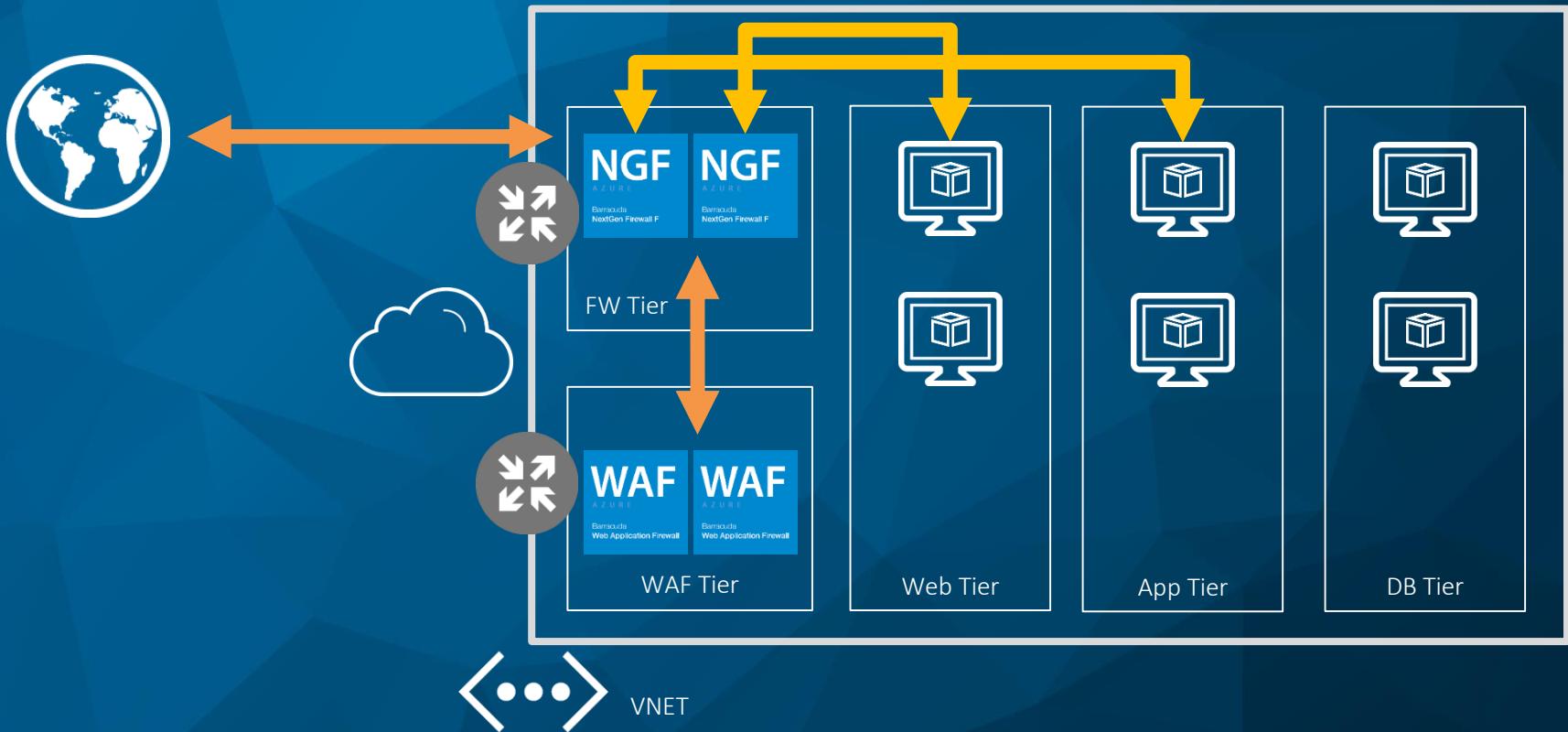
Cloud

Turn the “weakness” into strength

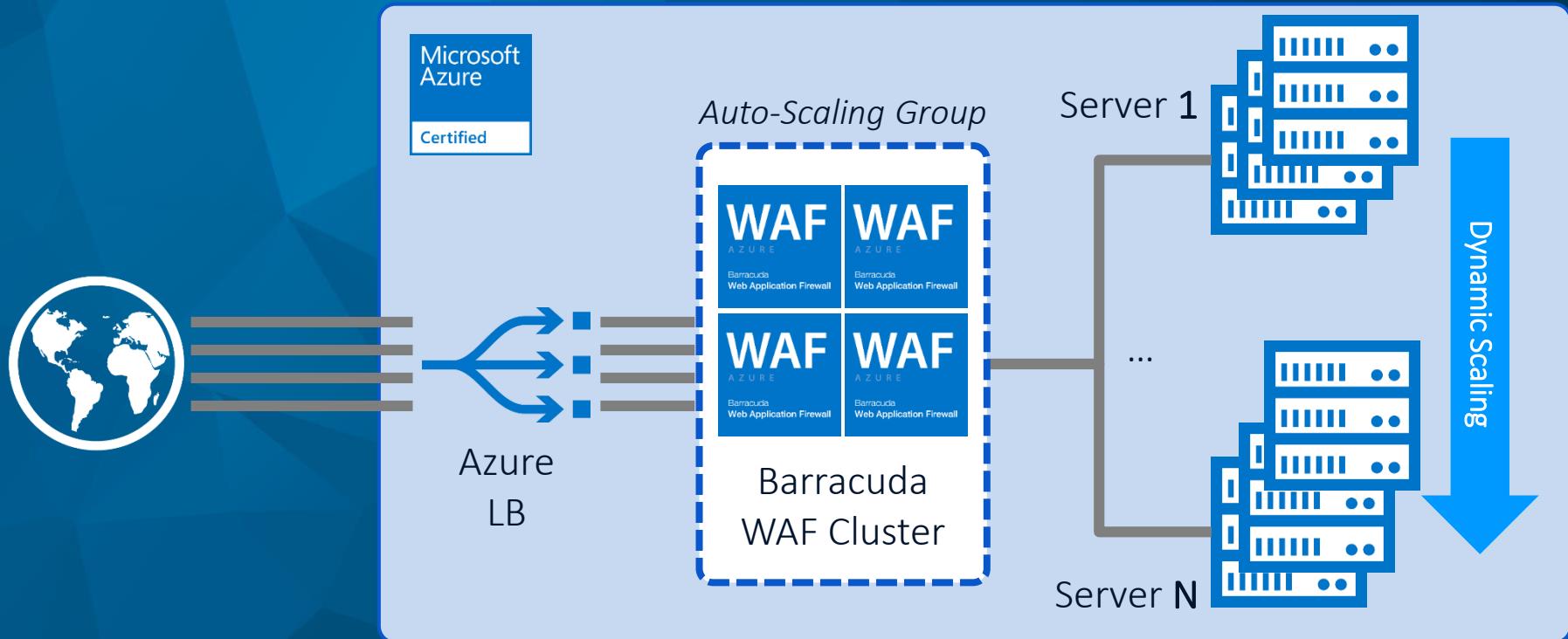
- Make use of the agility and flexibility for security measures
- Auto-scaling includes auto-firewalling
- All development and testing environments can have fully-fledged security
- Backup and restore at amazing speed



Deploying Multi-Tier Network Architectures



Dynamic Scaling; It's Different in the Cloud



Cloud – Essence

WTF!



Implications on Infrastructure Protection

Cloud

Things

Crime

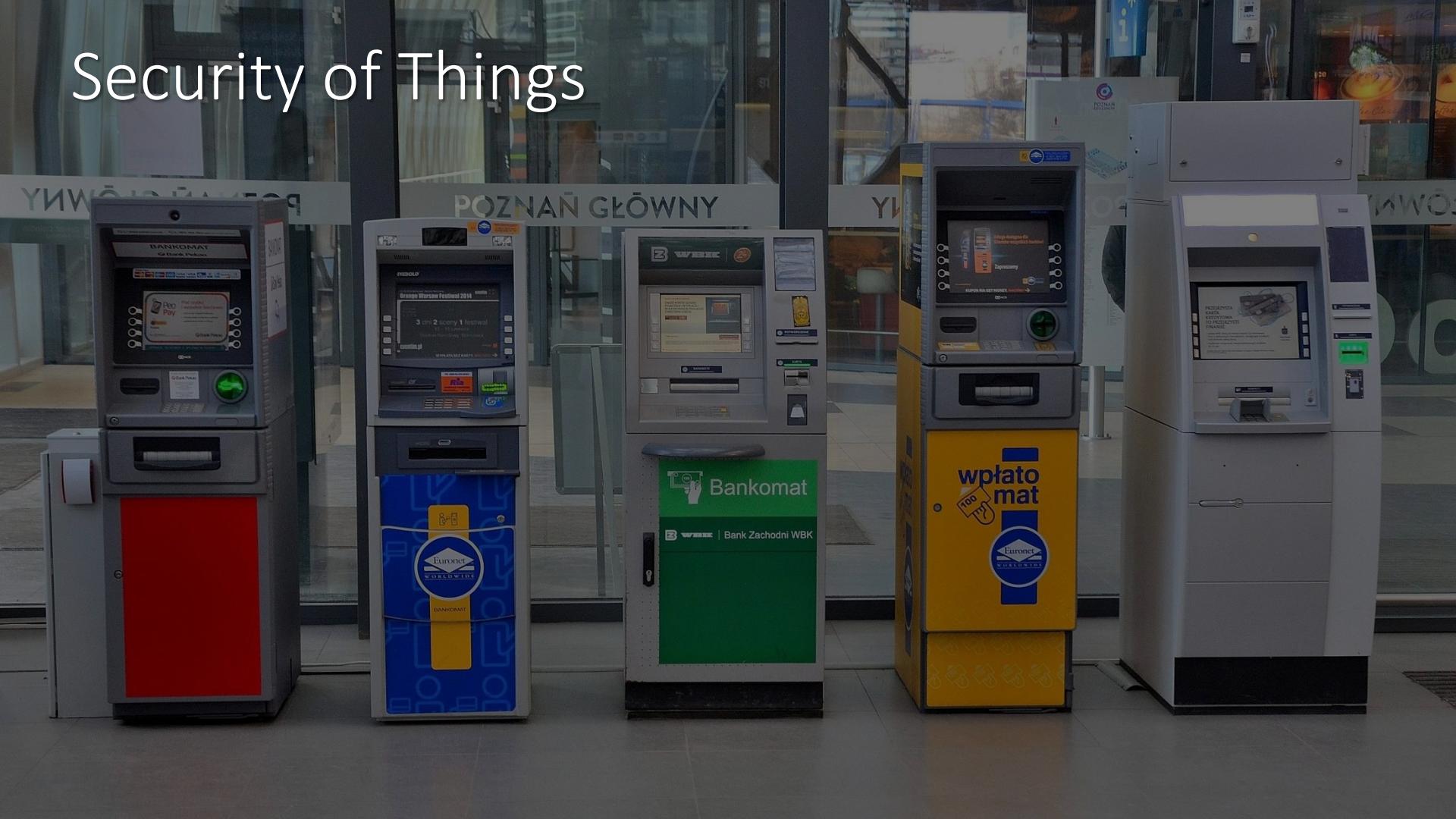
Threats



Security of Things



Security of Things



Security of Things



Größenabschätzungen für IoT



4 Billionen EUR

umfasst die Wertschöpfung mit IoT-Einsatz



50 Milliarden Dinge

(nicht Menschen) werden 2020 Internetverbindung haben (8 Milliarden in 2014)

Source: Cisco Whitepaper, Embracing the Internet of Everything To Capture Your of \$14.4 Trillion 2013, p15



Risikofaktoren

Business und Organisatorische Risiken

Gute alte IT Security Traditionen

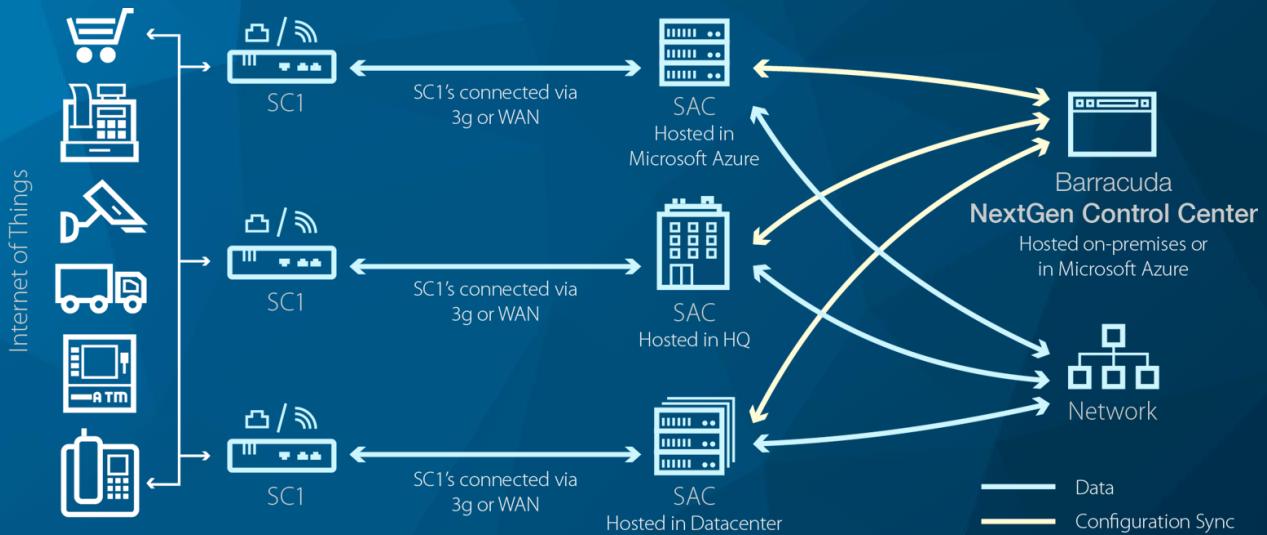
- Der Versuch und Irrtum Ansatz – ist im kleinen gefährlich, im Großen tödlich
- Schlampigkeit als Prinzip, Security als Zufall
- Reaktives Security Modell („Schau mer moi“)

Unterschätzte Elemente

- Die schiere Größe macht die obigen Ansätze zu echten Problemen



Barracuda Secure Connectivity Appliance (sc1)



Lessons Learned

Viele Szenarien, aber auch Gemeinsamkeiten

- Erhalt des privaten, nachweisbar internen Netzwerks
- Viele brauchen Hub für Kommunikation zu Kontrollinstanz (Datacenter)
- Deep inspection notwendig, aber nicht bei Maschine selbst

Existierende Firewalls sind oft nicht das Richtige

- Die skalierbare Architektur zählt, nicht nur das Gehäuse

Betriebskosten sind alles

- Zehntausend sind viel mehr als zehn. Viel mehr.



Things

Thesis 4

There will be more firewalls than iPads



Things – Essence

WTF!

Implications on Infrastructure Protection

Cloud

Things

Crime

Threats



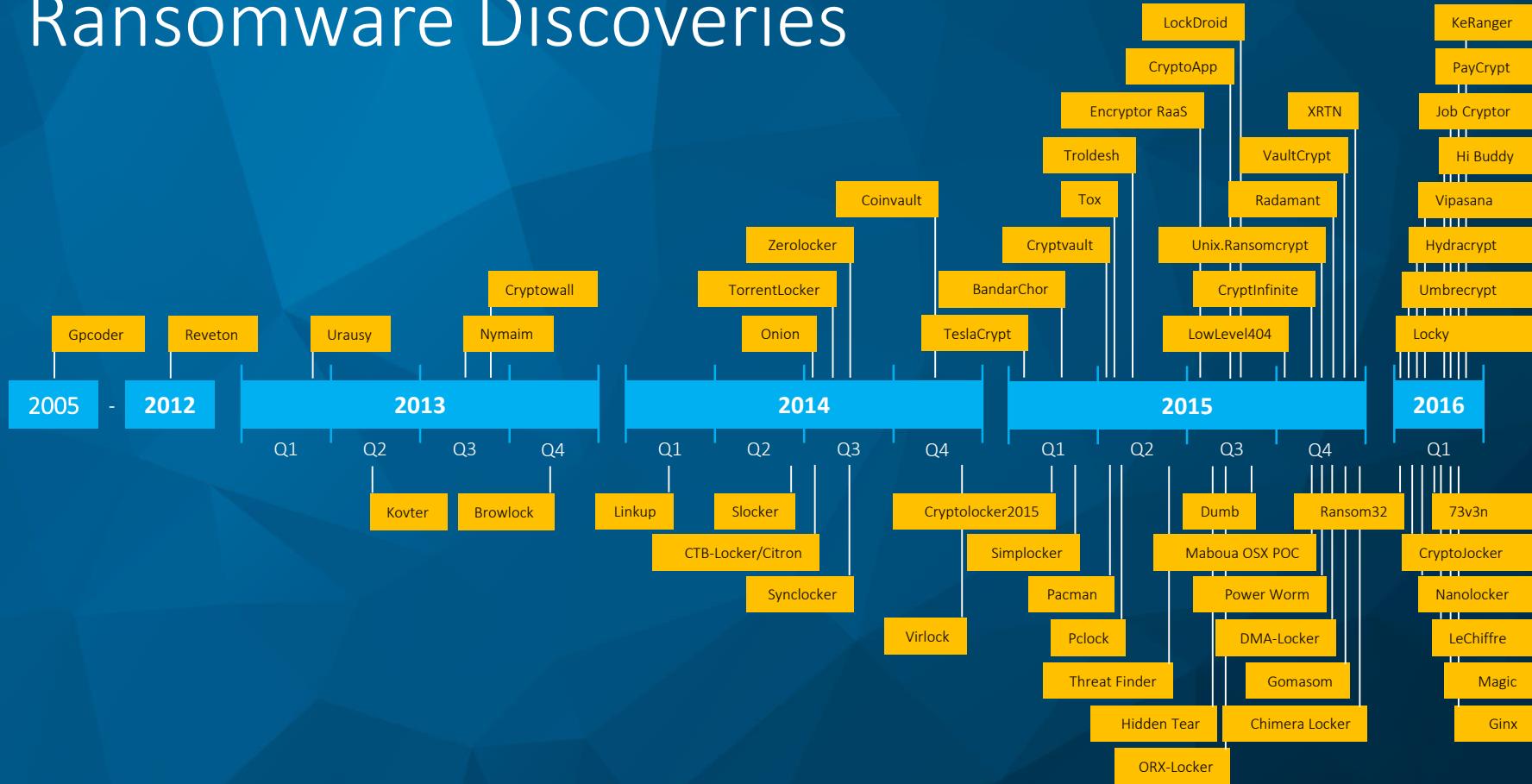


Crime?



Crime!

Ransomware Discoveries



Digital Transformation of Crime

	Technical Skills	Criminal Skills
Hacking	High	Medium
Advanced Threats	High	High
Ransomware	Medium	High
President's Fraud	Low	High



Digital Transformation of Crime

Thesis 5

No criminalization of
digital business
BUT: Digital
transformation of
criminal business



Crime – Consequences

Know your attack surface

Seal your attack surface



Crime – Essence

WTF!



Implications on Infrastructure Protection

Cloud

Things

Crime

Threats



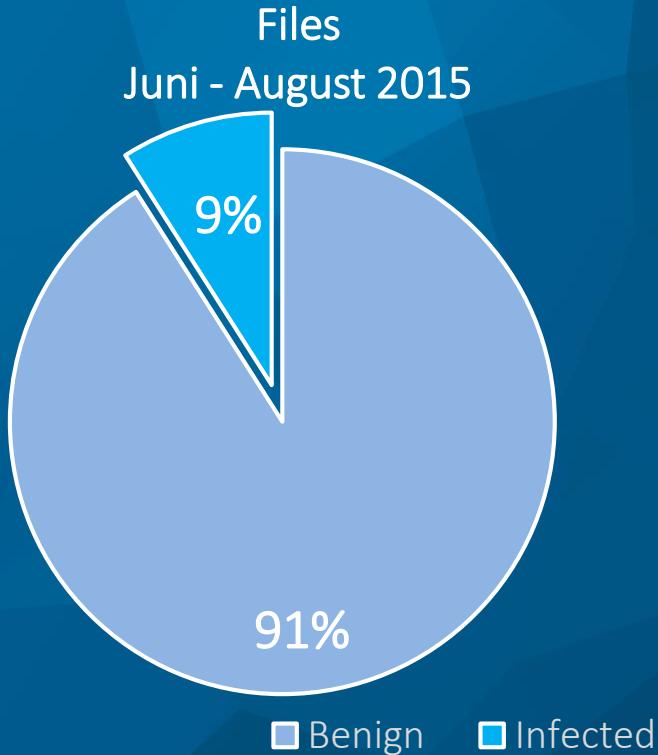
New Major Threat Vectors

Advanced Threats

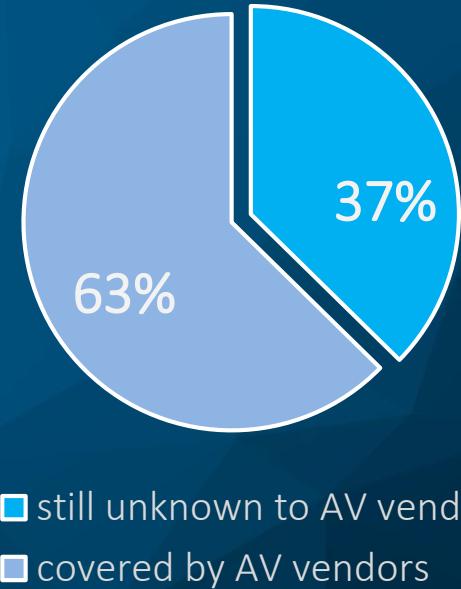
Ransomware



Behind the Scenes – Advanced Threats



AV detected Malware
6 months later?



Phishing Facts – Awareness works !?

23%

Of all users open phishing mail

11%

Of all users blindly open attachments



The Dangerous Ones - Cryptolocker

!!! IMPORTANT INFORMATION !!!

All of your files are encrypted with RSA-2048 and AES-128 ciphers. More information about the RSA and AES can be found here:
[http://en.wikipedia.org/wiki/RSA_\(cryptosystem\)](http://en.wikipedia.org/wiki/RSA_(cryptosystem))
http://en.wikipedia.org/wiki/Advanced_Encryption_Standard

Decrypting of your files is only possible with the private key and decrypt program, which is on our secret server. To receive your private key follow one of the links:

1. <http://6dbxqgam4crv6r6.tor2web.org/>
2. <http://6dbxqgam4crv6r6.onion.to/>
3. <http://6dbxqgam4crv6r6.onion.ca/>
4. <http://6dbxqgam4crv6r6.onion.ln1>

If all of these addresses are not available, follow these steps:

1. Download and install Tor Browser: <https://www.torproject.org/download/download-easy.html>
2. After a successful installation, run the browser and wait for initialization.
3. Type in the address bar: `6dbxqgam4crv6r6.onion/`
4. Follow the instructions on the site.

!!! Your personal identification ID: [REDACTED] !!!□18



TESLA CRYPT

All your important files are encrypted.

At the moment, the cost of private key for decrypting your files is 1.5 BTC ≈ 415 USD.
Your Bitcoin address for payment: 1JVR7hJ2wmdVrogHcd6fWMIEjRynMkWF2

\$ PURCHASE PRIVATE KEY WITH BITCOIN

You can also make a payment with PayPal My Cash Card

In case of payment with PayPal My Cash Card your total payment is 1,000 USD (2 PayPal My Cash Cards)

\$ PURCHASE PRIVATE KEY WITH PAYPAL MY CASH CARD

 PETYA
Ransomware

Start Payment FAQ Support English ▾

Your computer has been encrypted

The hard disks of your computer have been encrypted with an military grade encryption algorithm. It's impossible to recover your data without an special key. This page will help you with the purchase of this key and the complete decryption of your computer.

The price will be doubled in:

6 days 12 hours 9 minutes 18 seconds

[Start the decryption process](#)

You became victim of the PETYA RANSOMWARE?

The harddisks of your computer have been encrypted with an military grade encryption algorithm. There is no way to restore your data without a special key. You can purchase this key on the darkest page shown in step 2.

To purchase your key and restore your data, please follow these three easy steps:

1. Download the Tor Browser at "<https://www.torproject.org/>". If you need help, please google for "access onion page".
2. Visit one of the following pages with the Tor Browser:
<http://petya37h5tbbuyvki.onion/MonHQz>
<http://petya5koahsf7sv.onion/MonHQz>
3. Enter your personal decryption code there:
`afMr5Z-C83M2q-Nv9uR1-g96ZXY-a4iu47-c5R4iT-xR1W2k-nX4HmW-rnc1Kg-HMckdy-WBWRr-rXz6Tz-j069hJ-prc5Ry-Myg9rt`

If you already purchased your key, please enter it below.

Key: _____

Threats – Essence

WTF!



What to Remember



IT will move from CFO to CEO



IT will become de-localized



Cloud-based IT will be more secure than on-premises (if you want to)



“Things” will multiply the number of firewalls



Digital transformation of crime



Firewalls, Email-Security, Backup are the
Secure Trinity



Essence

WTF!

Thank You

