Why perimeter security is coming to an end

Elmar „mc.fly“ Lecher

Security advisor at the

Port of Rotterdam

Elmar „mc.fly“ Lecher

- Hacker
- Security professional
- NPC
- Hackerspace
- Woodworker

Elmar „mc.fly“ Lecher

- Started in the BBS age
- hacker scene since 1996
- sec conference speaker since 1999
- Computer professional since 2003
- Security professional since 2011
- Netherlands since 2016

Elmar „mc.fly“ Lecher

- Linkedin: elmarlecher
- Mastodon: @mcfly@chaos.social
- Matrix: @mc.fly:milliways.info

Motivation for the talk

As a network engineer and later security professional I have build a lot of security solutions based on the perimeter.

We got better and more complex technology.

It did not help.

Motivation for the talk

On the 27th of June 2017 the company I worked for got pwned by notPetya.

Within 8 minutes most of the company network was gone.

Motivation for the talk

Events like these let you think if the solution you have is still he right solution.

Change

Not only technology and ways of working change.

Also principals of the ICT world need to change.

This talk is about this change.

What is a perimeter

Wikipedia:
“A perimeter is a closed path that encompasses, surrounds, or outlines either a two dimensional shape or a one-dimensional length.“

What is a perimeter

A line that defines an inside and and outside

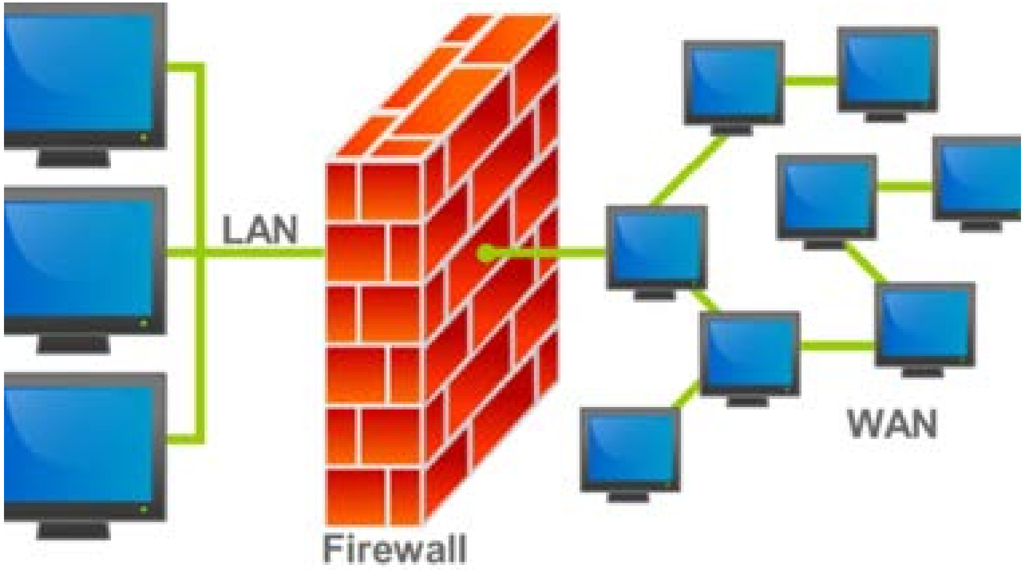
Think a castle with walls and a gate

What is a perimeter

The outside network

gateway

the inside network



Evolution of computer networks

Mainframes

Big machine, sits in a room built for it.

Perimeter is the room, the gate is the door.

- Terminals
- Modems
- X.25

Mainframe

Mainframe

Mainframe

This was the first moment when computers were connected.

The main risks were Kids that wanted to play Chess and Thermonuclear war.

Client server network IPX

Network typically in a building.

Perimeter was the building doors.

- Protocol Novell Netware
- Shares files and printers

Client server network TCP/IP

Still in a building, just with newer technology

For example

- Novell Netware 4.x
- Windows 2000 server
- linux samba / lamp server

Shares files and printers

Client Server applications

Applications were being used by more than one user.

We got client server applications.

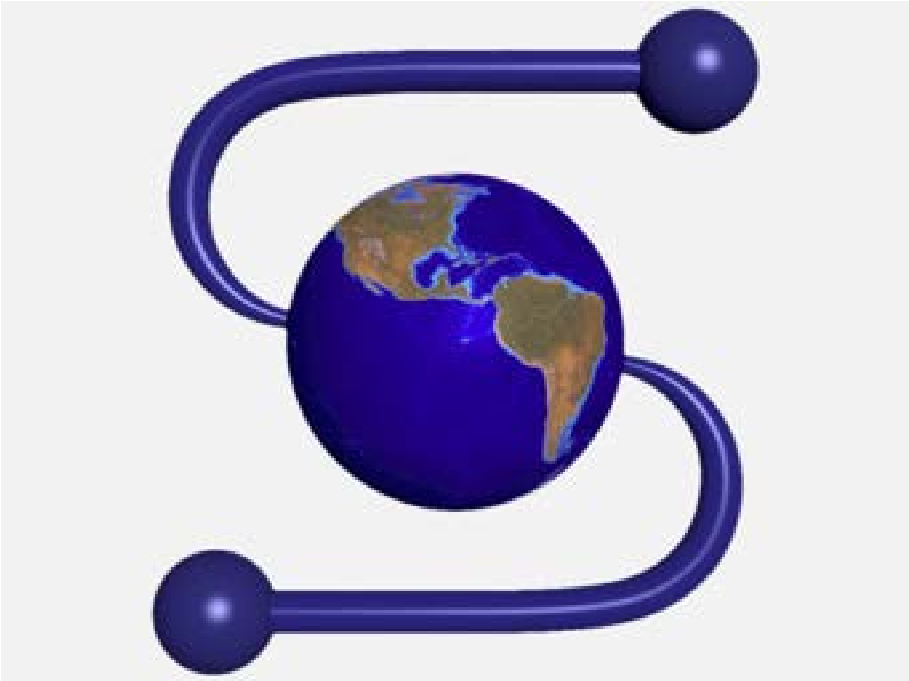
Client Server applications

A client application on a desktop of a user talks to a server application on one of the servers.

TCP/IP network with internet

And suddenly

the Internet



TCP/IP network with internet

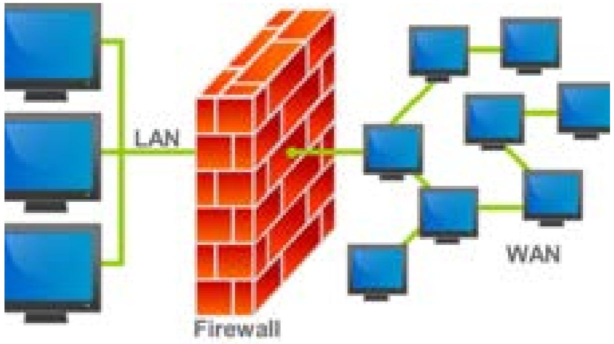
And suddenly

the Internet

(according to the it crowd)

Firewalling

The company network was now connected to the Internet aka a public network



Firewalling

This is the moment where firewalls as the gates of perimeter security became important.

Check Point
SOFTWARE TECHNOLOGIES LTD.

Intranet applications

Intranet applications became common replacing desktop applications

We still use those, we just call them different.

Often main application here: HR (SAP)

External Datacenters

The servers were moved from the „Basement“ of the company to a datacenter.

The company office network was connected to the datacenter network

External Datacenters

The physical and the network boundaries became detached.

Networks became separated into VLAN’s – virtual networks within the company.

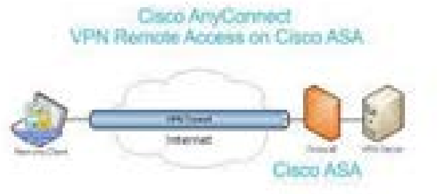
External Datacenters

The network perimeter now extends from the company building(s) to the datacenter.

There were multiple gates connecting the virtual networks within the company.

VPN

First people had to be connected from their Laptop to the company network to connect to Intranet services



VPN

Now computers all over the world were part of the company network and were within the perimeter

Intelligent firewalls

Firewalls as the gates evolved too.
We got Application firewalls.

IDS/IPS systems
SSL interception
user aware firewalls

Software as a service

Intranet applications moved into the internet and became cloud applications

Software as a service

We tried to include those services into the perimeter by restricting access to them to the company network and identities.

Platform as a service

Servers in the Data center moved into the internet and became cloud platforms

Platform as a service

The Servers in the cloud data centers became part of the company network.

They also were within the perimeter in their own virtual networks

Infrastructure as a service

We tried to include all of the virtual cloud services into the company perimeter

Infrastructure as a service

The whole datacenter and most company ict-services moved into the internet and became cloud Infrastructure

Work from Home

Due to covid most of my employees were forced to work from home.

Work from Home

We connected all the workers via VPN to the company network.

The perimeter now contained the home networks of the employees

And the coffee places where they hang out

And their coworking spaces.

Evolution of computer networks

The company perimeter looked very „interesting“ meanwile.

That’s where we are today.

Compliancy

The perimeter network is a cornerstone of most of the infosec compliancy frameworks.

Compliancy

The perimeter network is a cornerstone of most of the infosec compliancy frameworks.

It has served us well over the years.

Compliancy

The perimeter network is a cornerstone of most of the infosec compliancy frameworks.

It has served us well over the years.

This is also true for 2 other aspects that i will be mentioning also later.

problems of perimeter security

problems of perimeter security

Defining a useful perimeter sounds easy as concept but it gets really complicated.

problems of perimeter security

Defining an inside and an outside often leads to less tight security on the inside.

In the end that’s the idea of the protected area.

problems of perimeter security

If you imagine the perimeter trying to span over the office building, the cloud services, the VPN’s…

That means there is connectivity betwen them.

problems of perimeter security

The less tight security on the internal network made lateral movement by malware easier.

“we block all the traffic that is not defined as useful traffic“

problems of perimeter security

“we block all the traffic that is not defined as useful traffic“

Easier said then done….

problems of perimeter security

“we block all the traffic that is not defined as useful traffic“

Easier said then done….

Especially on a windows network.

Related developments

There are other developments that are not strictly perimeter security developments but that are connected….

User Management

company networks often also have a centralized User Management.

They used to require a perimeter security network.

Windows Server
Active Directory

User Management

Next to the local user management on the machine there are now also an additional users….

Windows Server
Active Directory

User Management

Next to the local user management on the machine there are now also an additional users….

Windows Server Active Directory

With very elevated rights…..

Company computer fleets

Installing large ammounts of alike computers is done using images.
That ensures every computer is like the others.

Company computer fleets

Installing large ammounts of alike computers is done using images.
That ensures every computer is like the others.

Same setups. The goal is identical computers

Company computer fleets

Installing large ammounts of alike computers is done using images.
That ensures every computer is like the others.

Same setups. The goal is identical computers

Same localadmin password

The unholy trinity

Supposed to help ...

- Perimeter network security
- Centralized user management
- Identical computers

The unholy trinity

The perimeter security created connectivity to other systems.

This enabled lateral movement.

The unholy trinity

Centralized user management ment that the same accounts existed on multiple machines.

This ment users compromised on one system could easier be compromised on other systems.

The unholy trinity

Installation over images resulted in identical systems that made debugging easier.

This also ment that exploitation on multiple machines is easier.

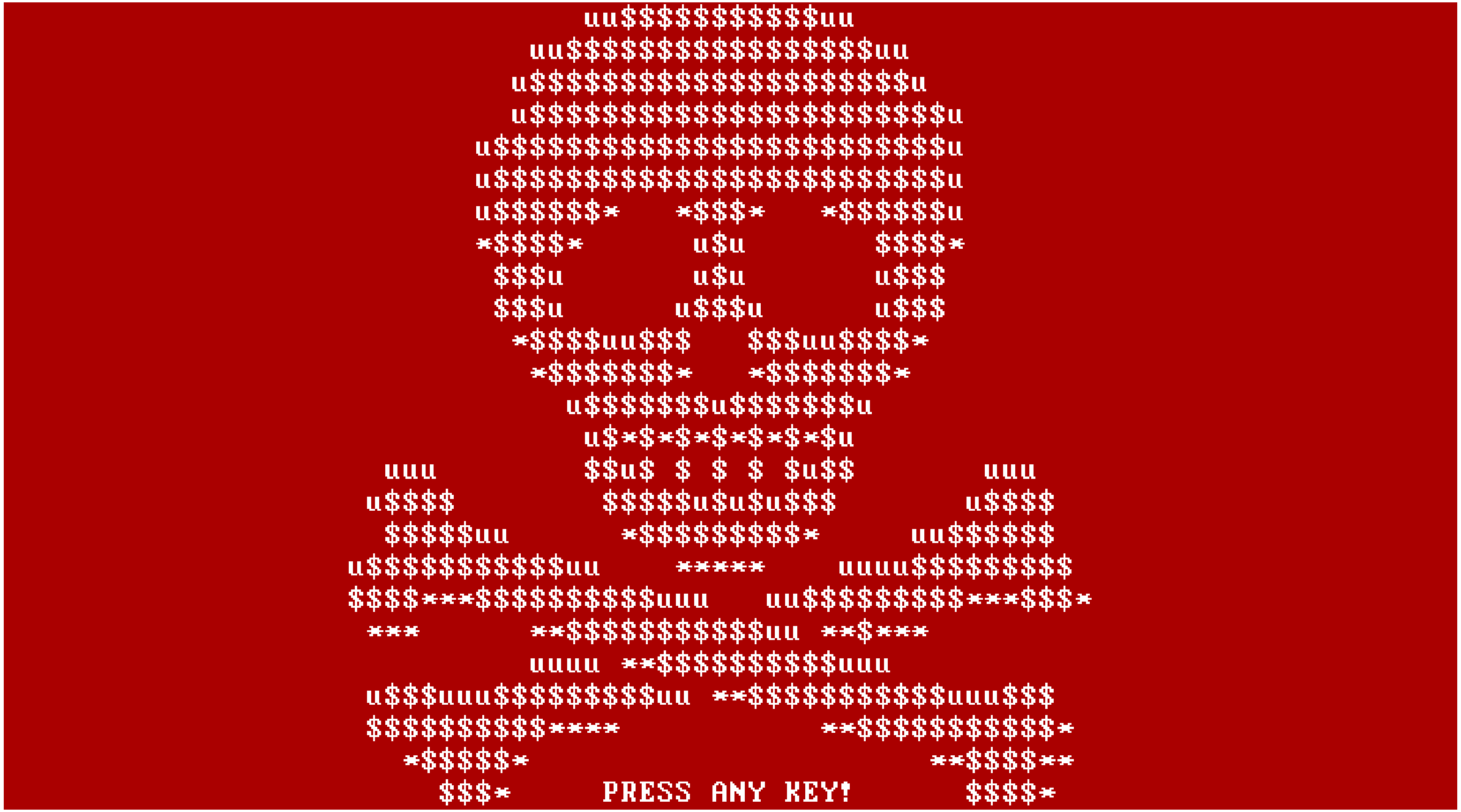
The unholy trinity

We have created an unholy trinity.

Ransomware started exploiting that on a large scale around 2015

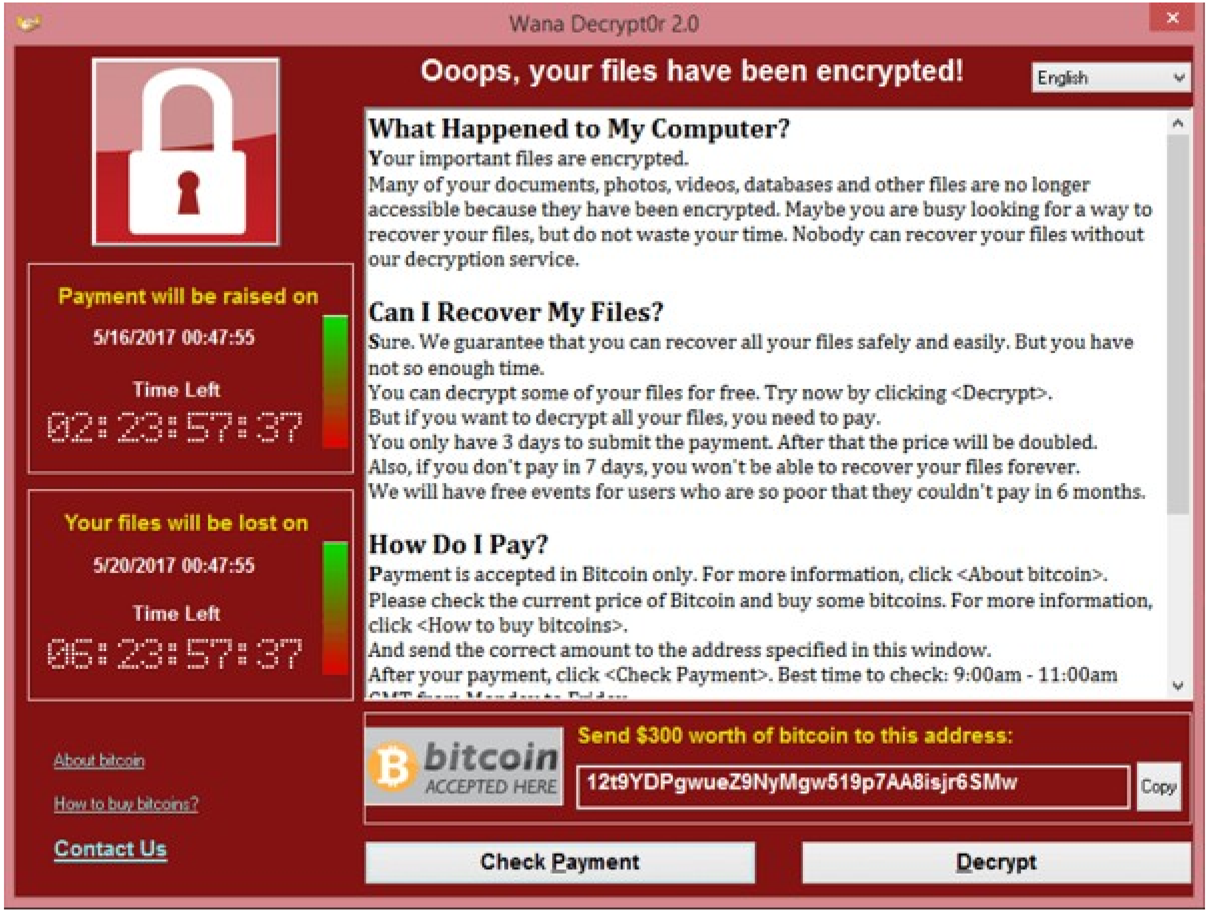
malware

Petya 2016



```
             uu$$$$$$$$$$$uu
          uu$$$$$$$$$$$$$$$$$uu
         u$$$$$$$$$$$$$$$$$$$$$u
         u$$$$$$$$$$$$$$$$$$$$$$$u
       u$$$$$$$$$$$$$$$$$$$$$$$$$u
       u$$$$$$$$$$$$$$$$$$$$$$$$$u
       u$$$$$$*   *$$$*   *$$$$$$u
       *$$$$*      u$u       $$$$*
        $$$u       u$u       u$$$
        $$$u      u$$$u      u$$$
         *$$$$uu$$$   $$$uu$$$$*
          *$$$$$$$*   *$$$$$$$*
            u$$$$$$$u$$$$$$$u
             u$*$*$*$*$*$*$u
  uuu        $$u$ $ $ $ $u$$       uuu
 u$$$$        $$$$$u$u$u$$$       u$$$$
  $$$$$uu      *$$$$$$$$$*     uu$$$$$$
u$$$$$$$$$$$uu    *****    uuuu$$$$$$$$$
$$$$***$$$$$$$$$$uuu   uu$$$$$$$$$***$$$*
 ***      **$$$$$$$$$$$uu **$***
          uuuu **$$$$$$$$$$uuu
 u$$$uuu$$$$$$$$$uu **$$$$$$$$$$$uuu$$$
 $$$$$$$$$$****           **$$$$$$$$$$$*
   *$$$$$*                      **$$$$**
     $$$*     PRESS ANY KEY!      $$$$*
```

WannaCry 2017



Ooops, your files have been encrypted!

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.

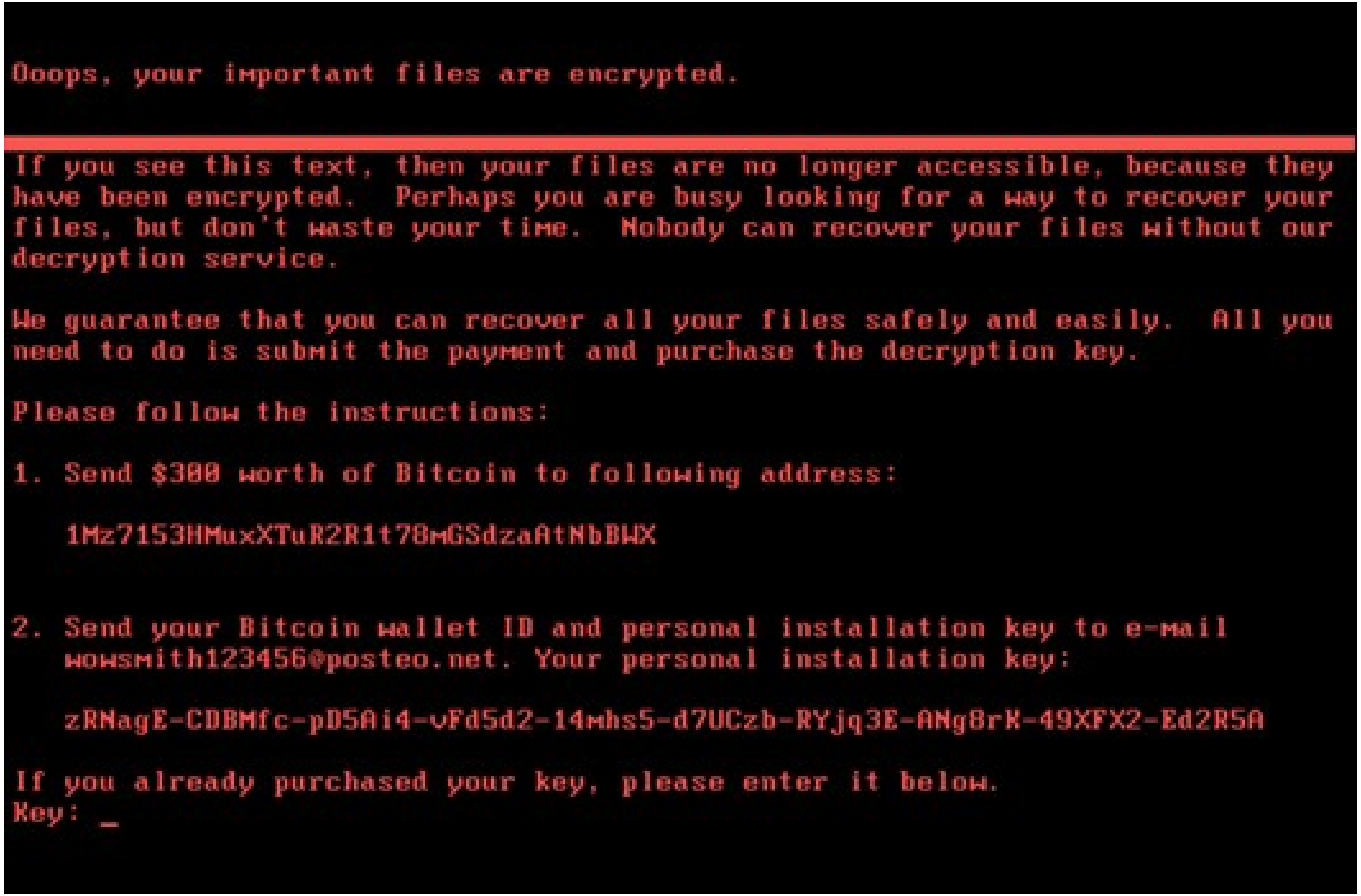
After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am GMT from Monday to Friday.

Send $300 worth of bitcoin to this address:

12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw

NotPetya 2017

- Maersk
- TNT
- DHL



```
Ooops, your important files are encrypted.

If you see this text, then your files are no longer accessible, because they
have been encrypted.  Perhaps you are busy looking for a way to recover your
files, but don't waste your time.  Nobody can recover your files without our
decryption service.

We guarantee that you can recover all your files safely and easily.  All you
need to do is submit the payment and purchase the decryption key.

Please follow the instructions:

1. Send $300 worth of Bitcoin to following address:

   1Mz7153HMuxXTuR2R1t78mGSdzaAtNbBWX


2. Send your Bitcoin wallet ID and personal installation key to e-mail
   wowsmith123456@posteo.net. Your personal installation key:

   zRNagE-CDBMfc-pD5Ai4-vFd5d2-14mhs5-d7UCzb-RYjq3E-ANg8rK-49XFX2-Ed2R5A

If you already purchased your key, please enter it below.
Key: _
```

complexity

complexity

The perimeter got complex.

complexity

The perimeter got complex.

the solutions are complex

complexity

The perimeter got complex.

the solutions are complex

complexity enables mistakes.

A way out

A way out

Zero trust

A way out

Zero trust

Never trust, always verify

Implement least privilege

assume breach

Zero Trust

Zero trust means you don’t give anyone in the company network a trust benefit based on ip addresses anymore.

The whole „internal“ network is to be treated like the internet.

Never trust, always verify

Never trust based on network ranges.

Verify user and devices accessing your data and ressources

Implement least privilege

Only grant rights needed to do the tasks effectively and no more

assume breach

Plan for breach of the systems

Have an incident response plan

Make the impact of an attack as small as possible.

Assume breach

Micro-segment your network ideally into applications

reduce dependencies whenever possible

Application security

Application security is critical

Application security

Application security is critical

but that’s its own talk of its own.

Strong encryption

Traffic on the network must be encrypted

Users and applications cryptographically & mutually verified

Strong encryption

A lot of users use only cloud software for their work.

Strong encryption

A lot of users use only cloud software for their work.

The reason why they need to be on the perimeter is gone

Backups

No need to explain this one I hope

Also: test the backup

migration

Ok, i see the point. But how to get there?

migration

Identify tools that are in the way of moving users out of the perimeter.

migration

Identify users that can be moved out of the perimeter network.

Move them out.

migration

Rinse and Repeat.

This will make the perimeter smaller and smaller and smaller.

Change

Not only technolog and ways of working change.

Also Dogmen of the ICT world need to change.

This talk was about this change.

Castles

I like the comparism of perimeter security and castles.

Castles

there's no castles used for defense anymore.

Castles

there's no castles used for defense anymore.

They are all museums.

Castles

or piles of rubble

most are piles of rubble.

Castles

you pick

The end

Questions?