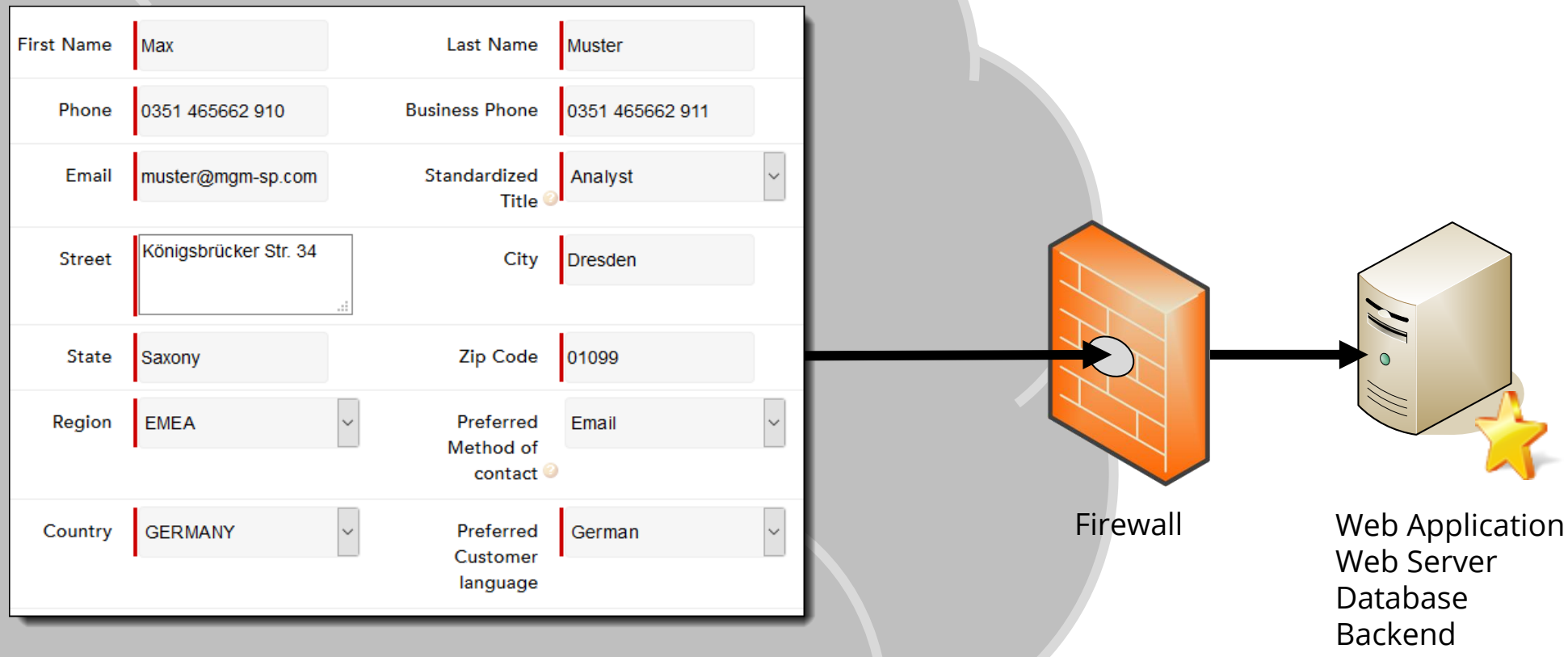
# Introduction

# What is (Web) Application Security?


mgm security partners
Gate25
No access !
Announcement:
This city is surrounded by a wall of the latest technology!
No conquest possible!
Gate80/443
Only for visitors of the market!
LEE DAE YOUNG

# What is Web Application Security

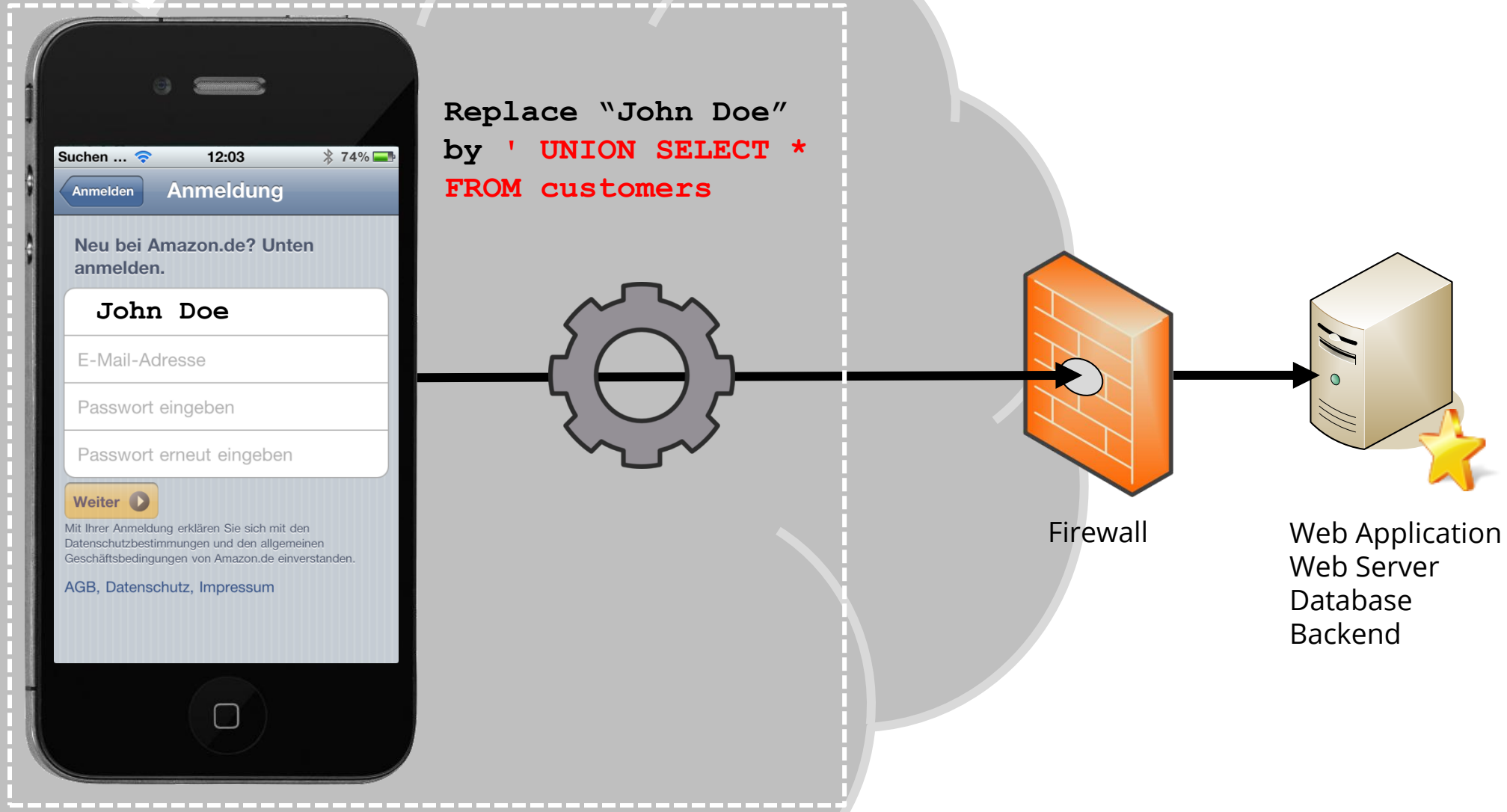
## Threats




**Low inhibition level:**
The attacker can always act hidden behind an anonymizing proxy from anywhere – next door and the other side of the world. There is almost no risk to be identified. All actions can be cancelled at any time.

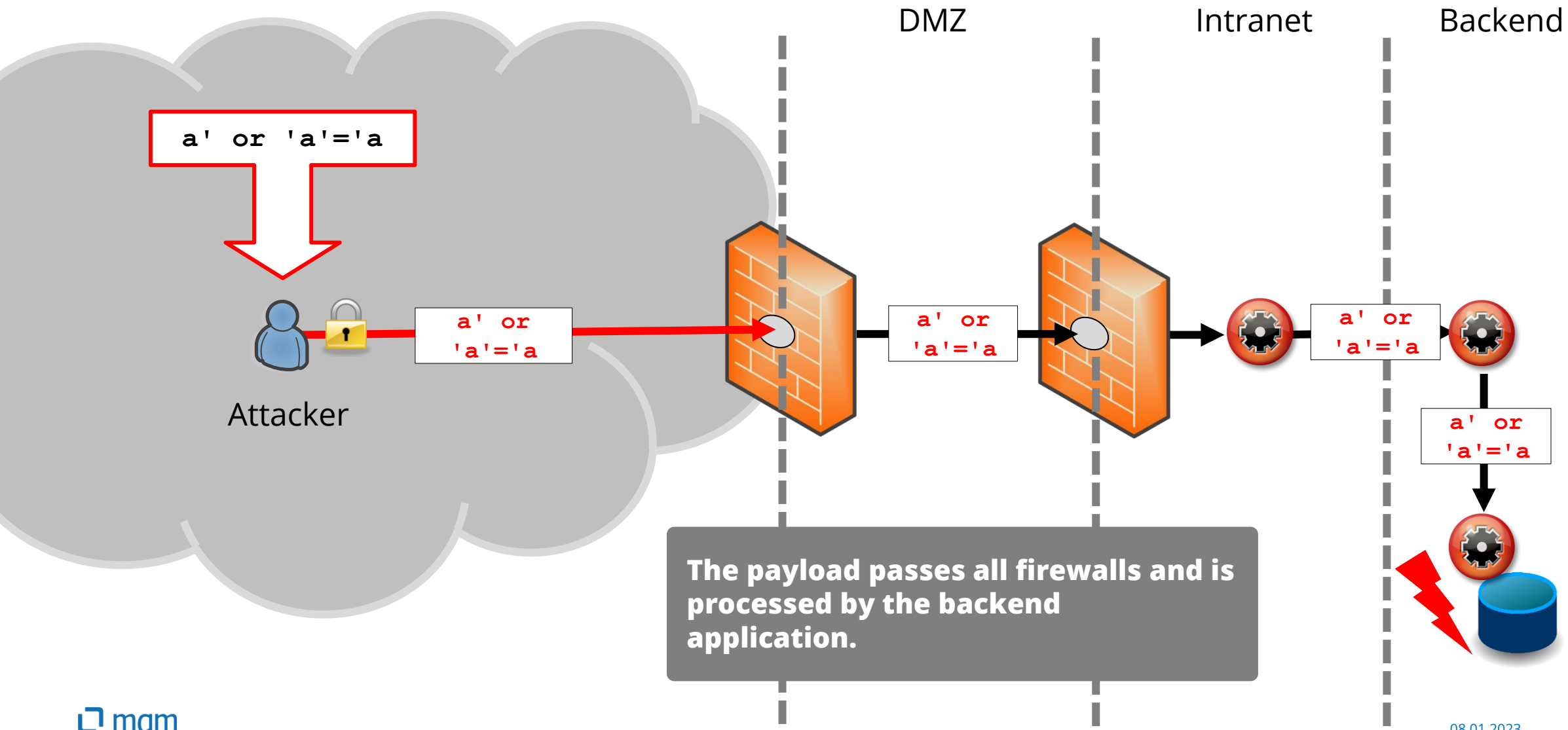
# What is Web Application Security

## Threats



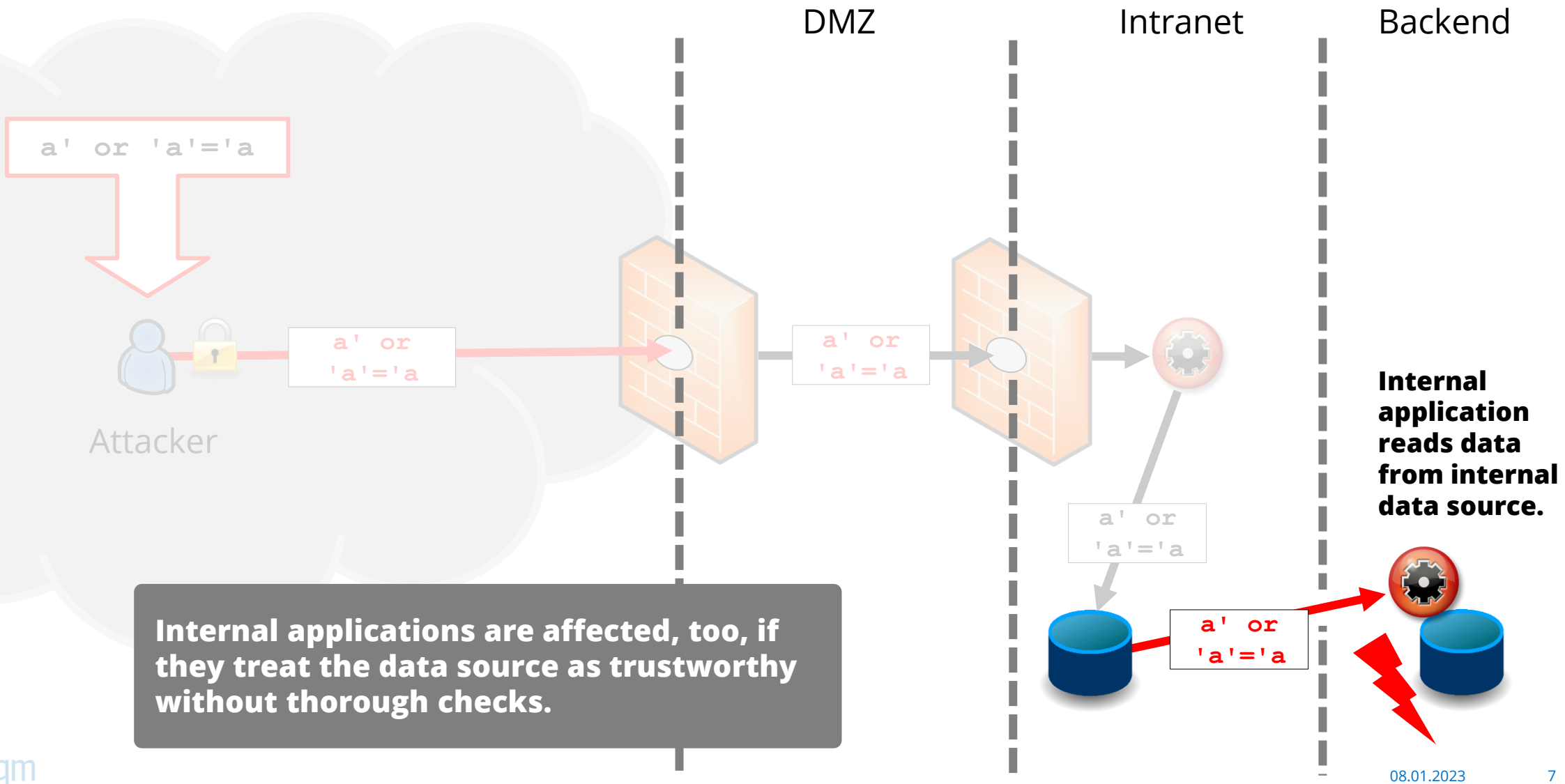
# Network Security does not help

... against Vulnerabilities on Application Layer (1)



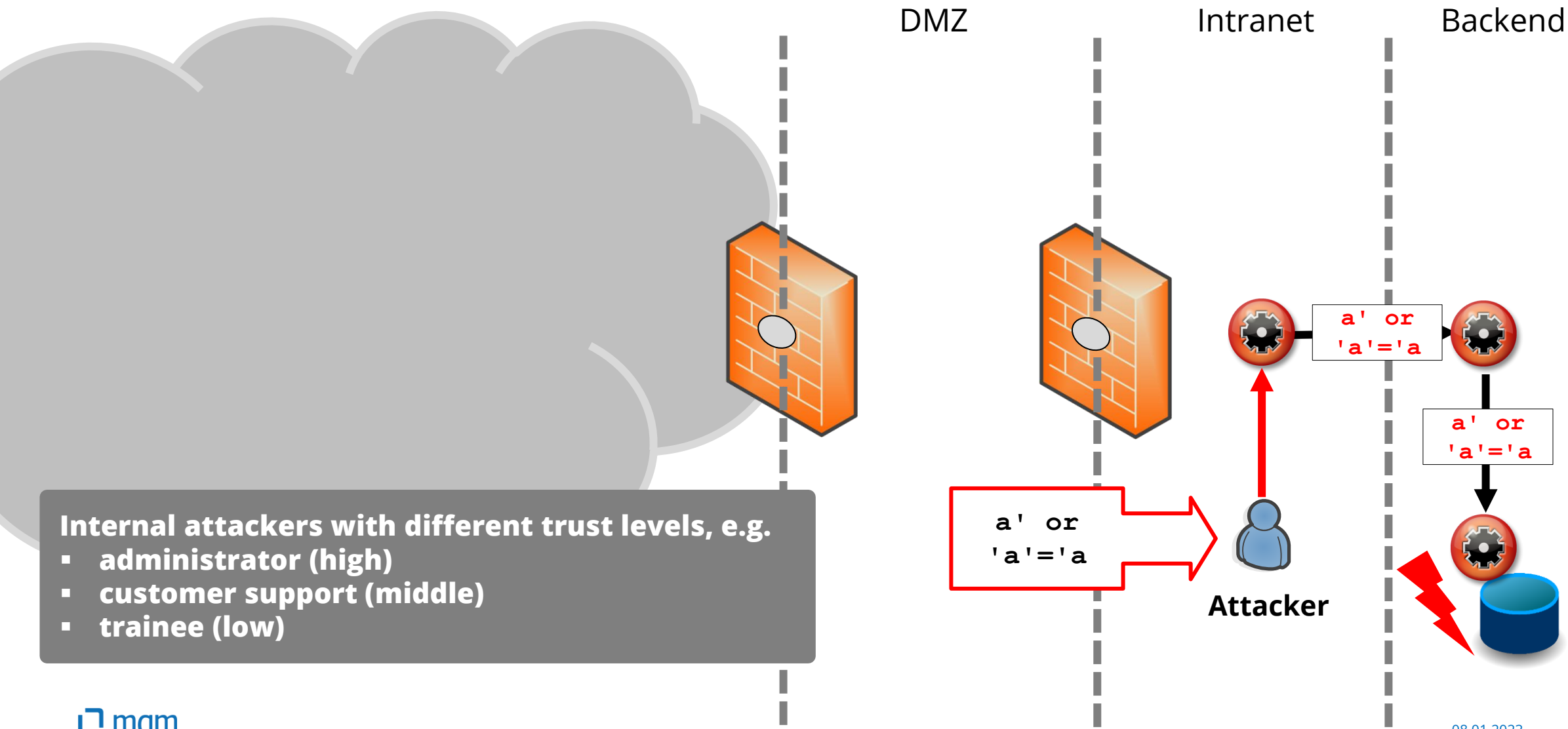
# Network Security does not help

... against Vulnerabilities on Application Layer (2)




**Internal applications are affected, too, if they treat the data source as trustworthy without thorough checks.**

# The Attacker can also be internal




**Internal attackers with different trust levels, e.g.**

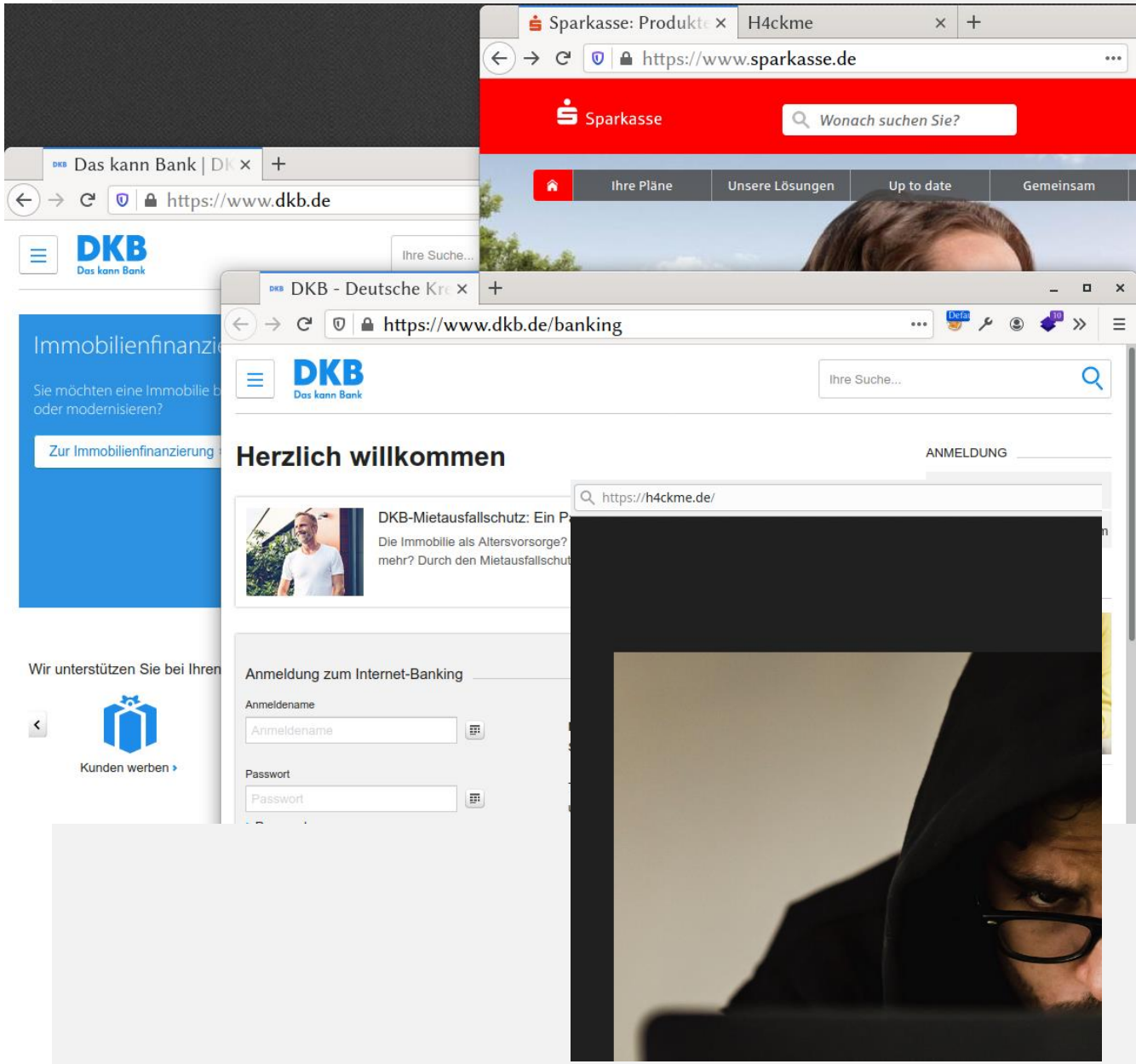
- **administrator (high)**
- **customer support (middle)**
- **trainee (low)**

mgm

# Web client vs. FAT client

# What does “Web-specific” mean?

- We use the same client for several purposes!
- Which site can interact with which?



# Why is it so hard to write secure Web Applications?

True Story

This is my son...

... in 2004 ...

# Why is it so hard to write secure Web Applications?

## True Story

When he was 14, he wanted to write a web application!

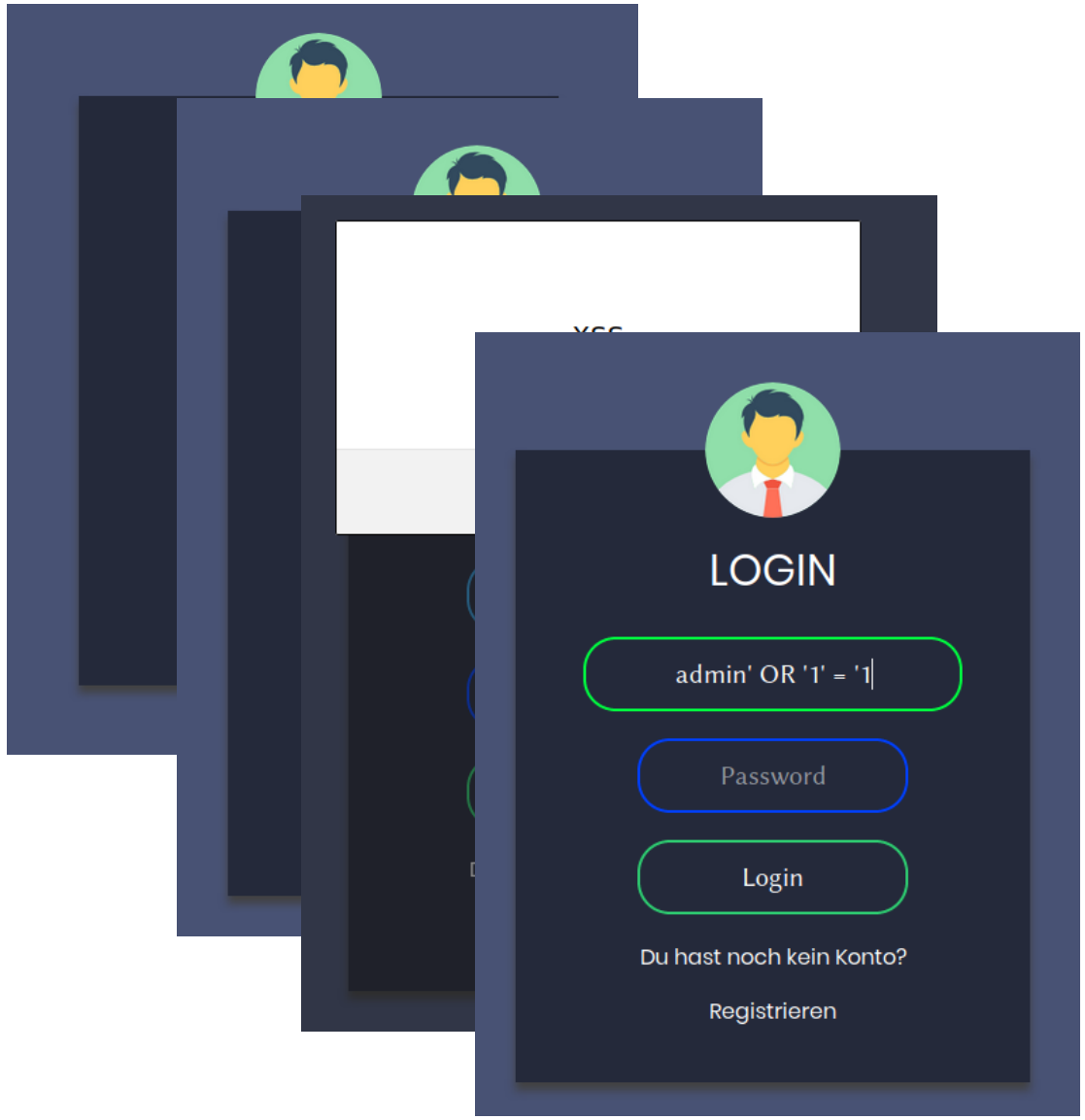
I said: No Problem, in terms of the web, your dad is a super-hero!

# Why is it so hard to write secure Web Applications?

True Story

- I let him program his first webpage
  - and explained how session fixation works…
  - … and username enumeration …
  - … XSS…
  - … SQLi…

- We discussed how to fix and prevent it
  - (remember, I am a super-hero ;-))



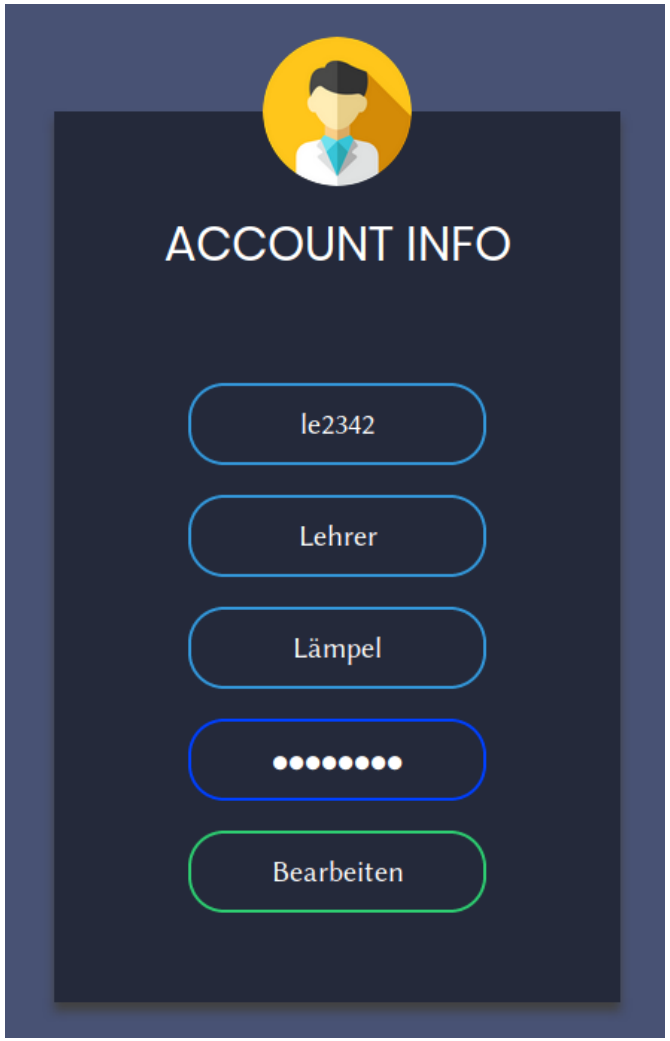
# Why is it so hard to write secure Web Applications?

True Story

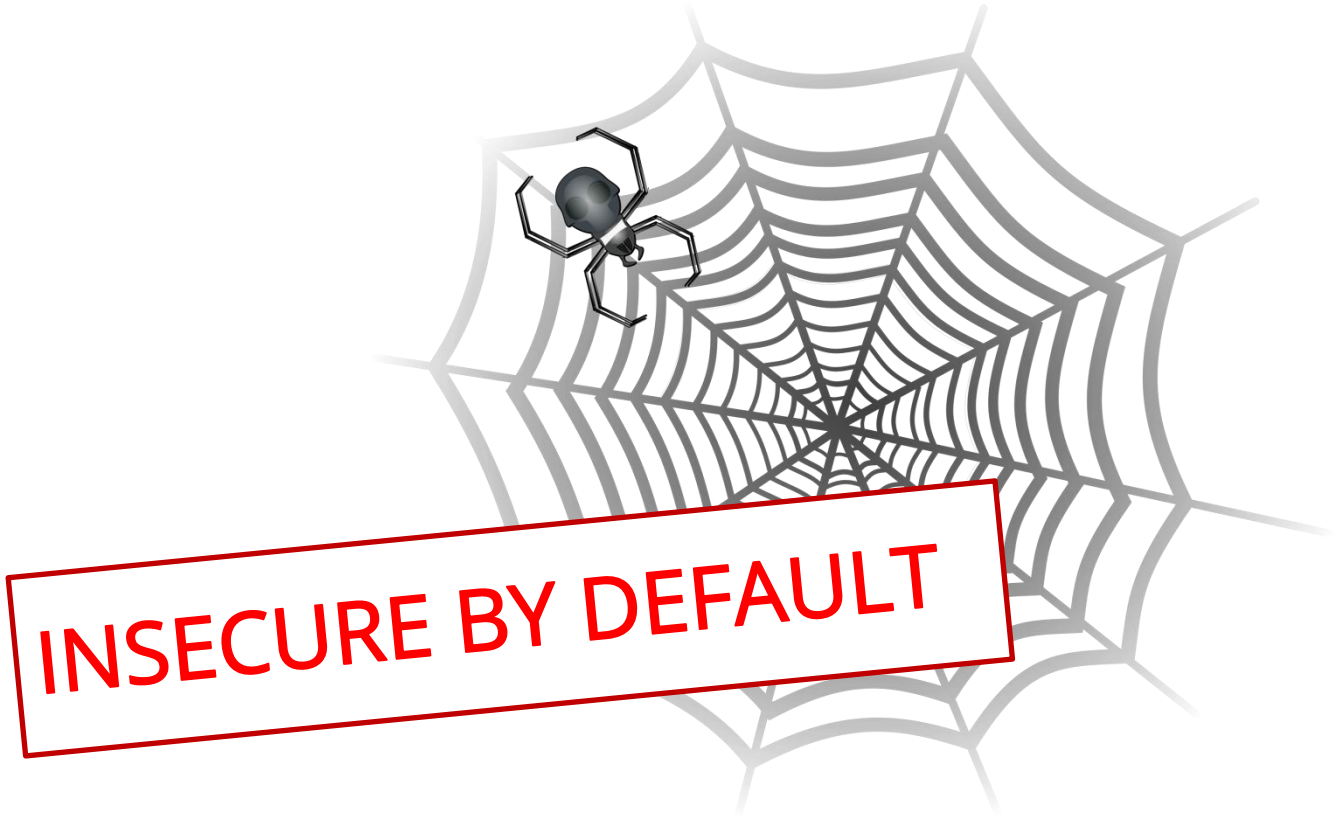
- The next day, he implemented another page on his own…

- Guess what…
  - 4 different SQLi
  - 1 second order SQLi
  - XSS on all fields

- and
  - passwords stored in plaintext
  - Cross-Site request forgery
  - missing re-authentication
  - a race condition leading to privilege escalation
  - sensitive data exposure

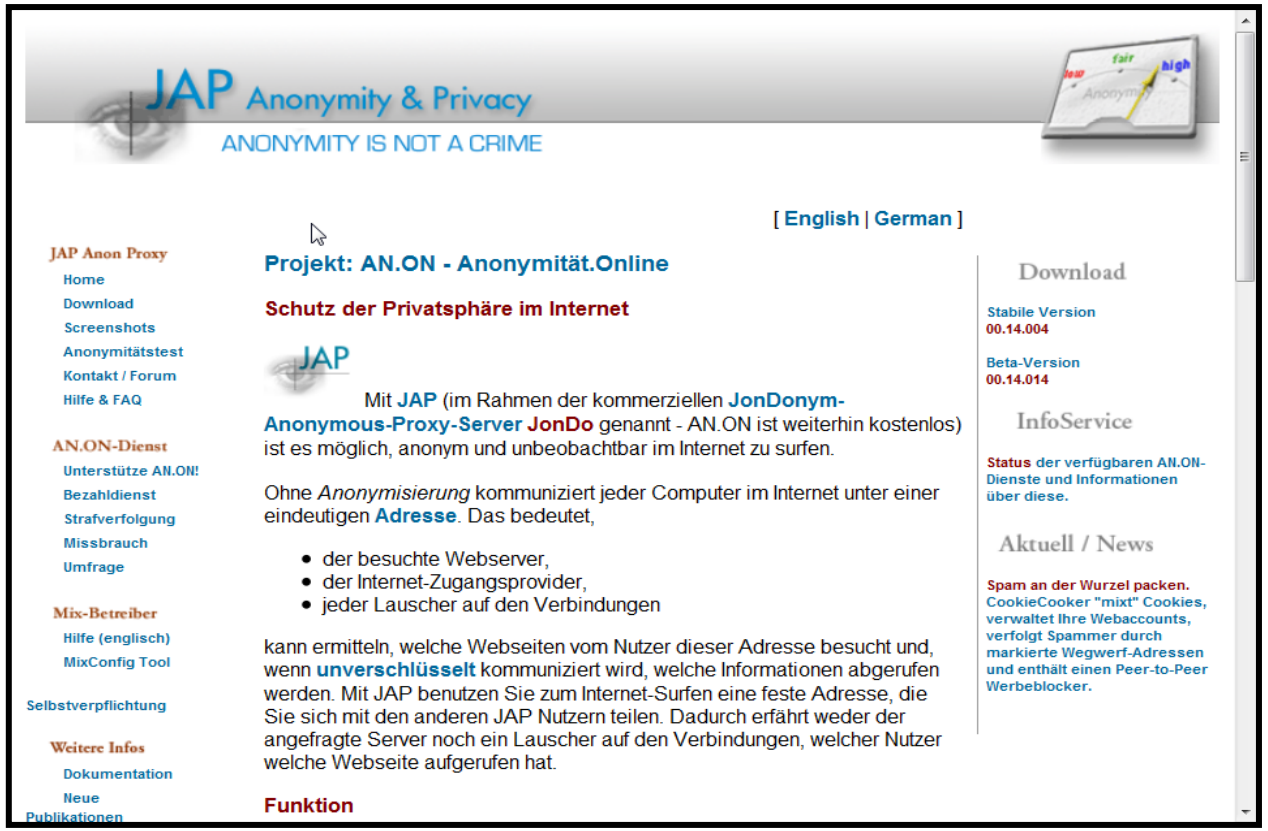


# Writing Web Applications...



# Anonymity in the Web

AN.ON / Tor

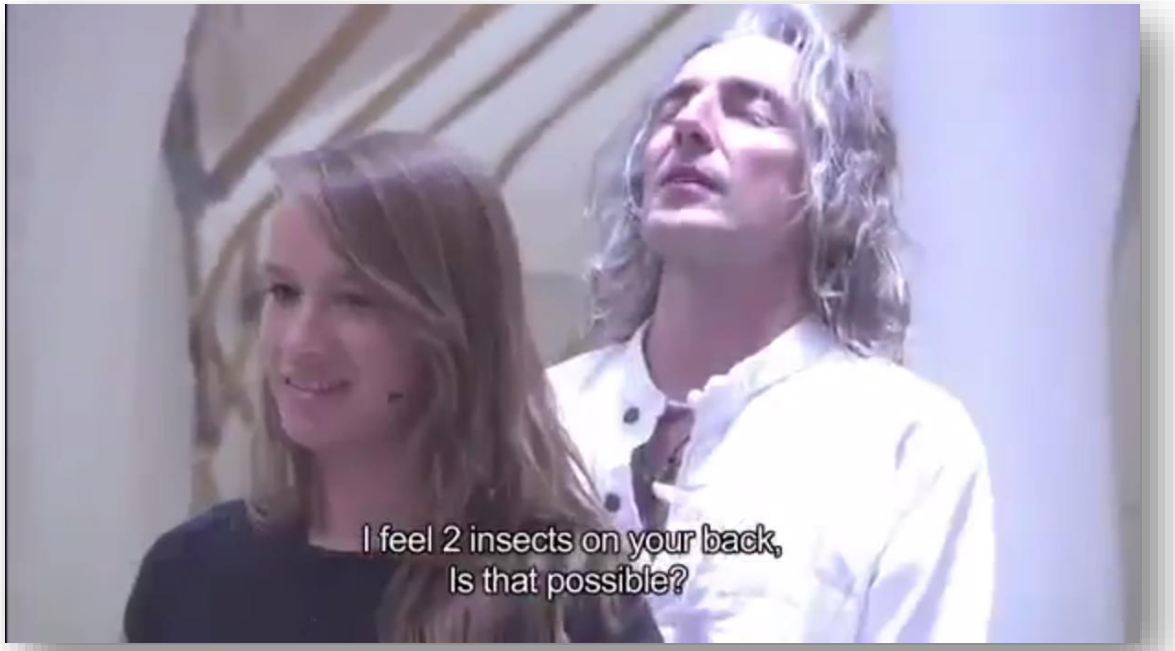



*https://anon.inf.tu-dresden.de*

*https://www.torproject.org/*

# This threat will increase permanently!

- https://www.youtube.com/watch?v=F7pYHN9iC9I

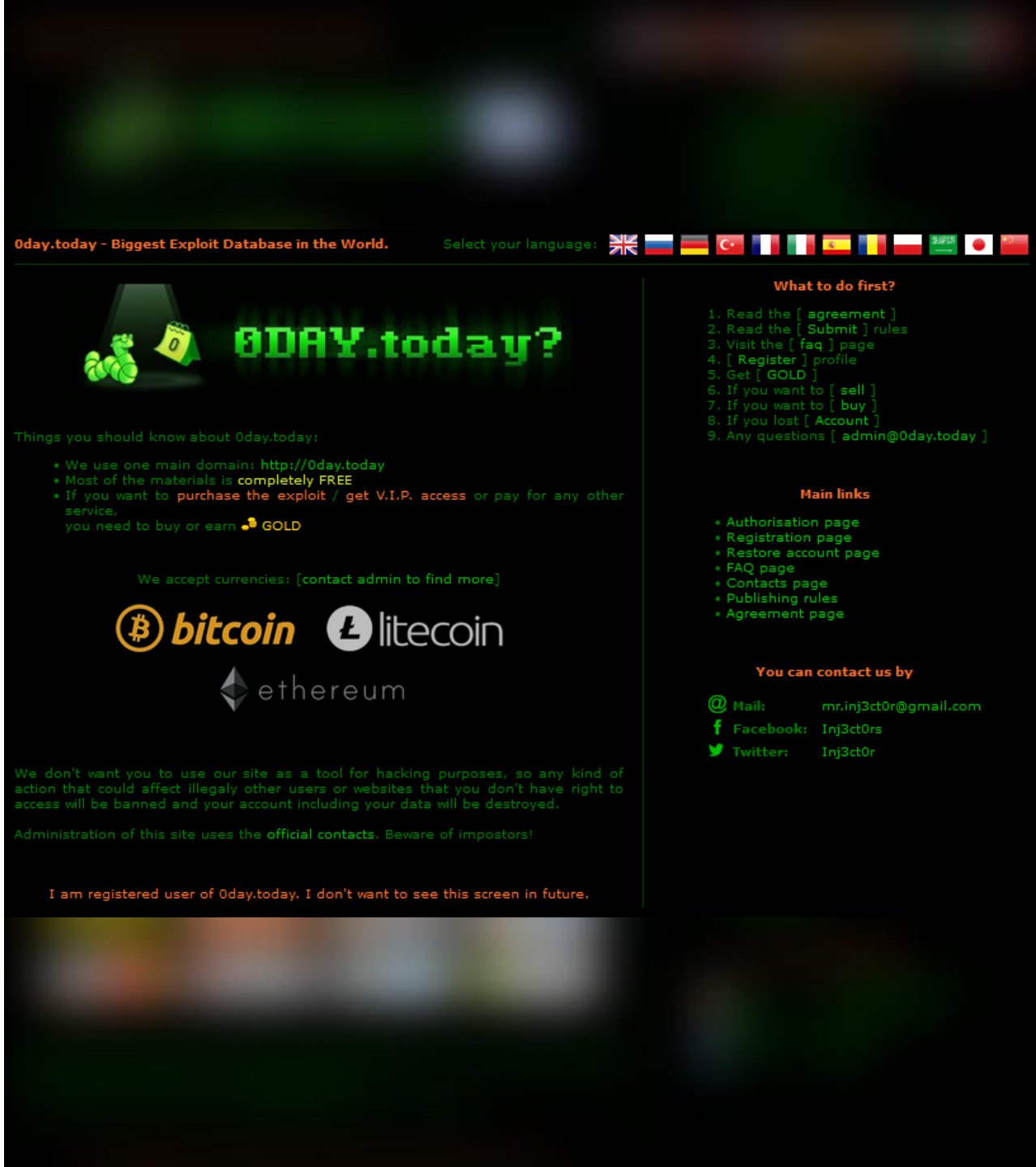



- How could this happen?
  1. Misusage of users
  2. Vulnerabilities in Web Applications

# Web Applications Security

## Current Situation

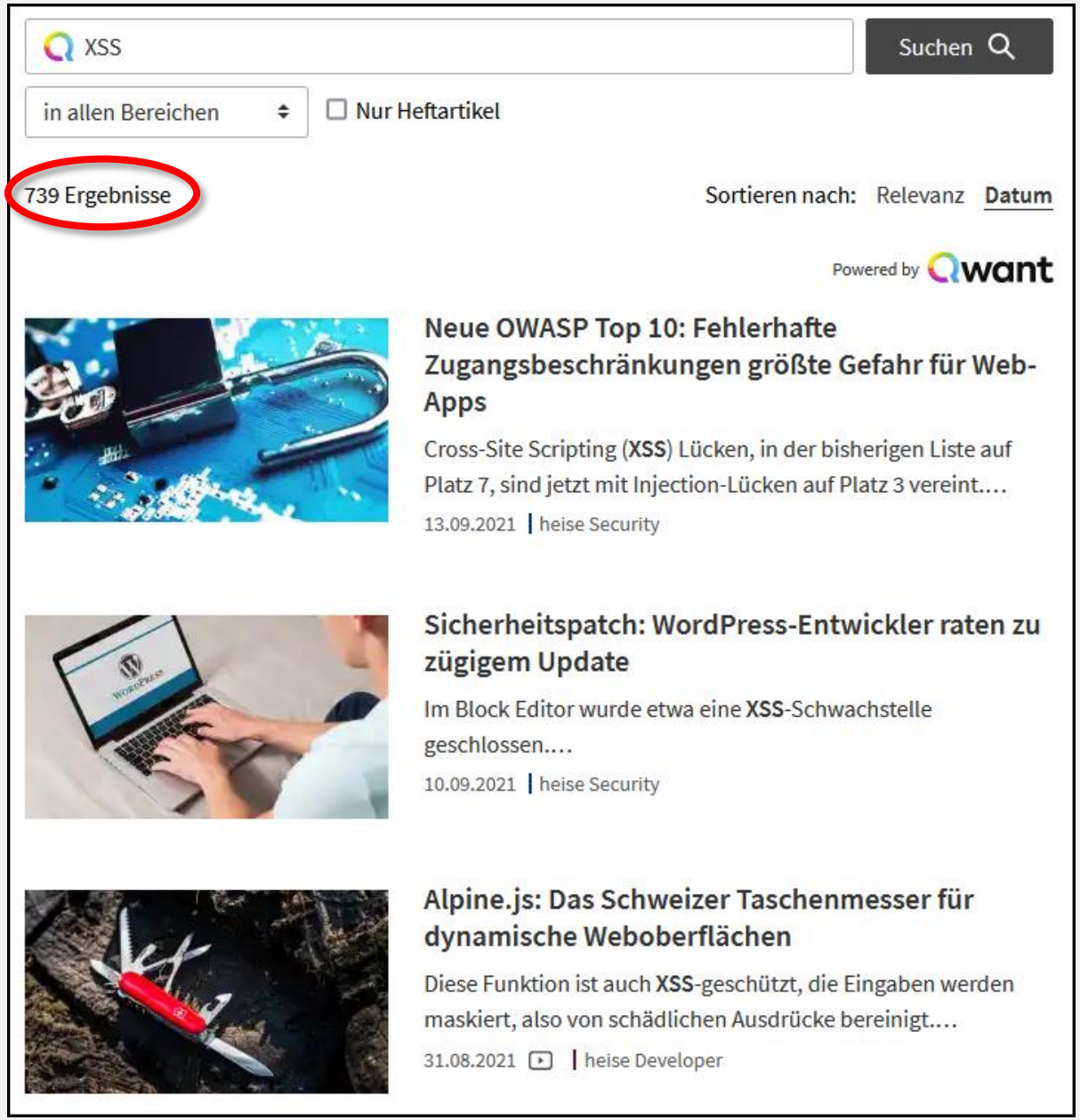
- OWASP: **80%** of all Web Applications have vulnerabilities
- Varonis Statistics 2020 (varonis.com):
  - **$3.86M** per breach (average)
  - **207 days** to identify breach
    - *280 days from identification to containment*
  - **58%** involving personal data
- Website hacking has become an **Underground Business**
  - Exploits & Vulnerabilities DB: *Inj3ct0r* (http://0day.today/)




mgm

# Current Situation (1)

- Attacks on Web Applications have **increased dramatically**
- **Example:**
  - Search for “XSS" at Heise Security




mgm

# Current Situation (2)

- **141% increase** in total number of records compromised (despite number of disclosed breaches shrank by 48%)
- **100% more** breaches including **ransomware**
- 5 breaches with **more than 1 billion** records lost
- mean breach severity increased from 4.75 in Q1 to **5.71 in Q4**
- a significant number of those breaches were **web-based**

LOHRMANN ON CYBERSECURITY

## 2020 Data Breaches Point to Cybersecurity Trends for 2021

As the COVID-19 pandemic grabbed 2020 headlines, the list of data breaches in government and the private sector quietly grew. And then came SolarWinds. What's next?

January 22, 2021 • Daniel Lohrmann, Dan Lohrmann

Risk Based Security released their 2020 year-end data breach report this past week, and despite an overall decline in breach events (security incidents), the number of breached records grew dramatically.

Other trends included a doubling of ransomware attacks from 2019 to 2020, and data breach severity rising.

Dan Lohrmann

Building effective virtual government requires new ideas, innovative thinking and hard work. From cybersecurity to cloud computing to mobile devices, Dan discusses what's hot and what works.

BIO / CONTACT / RSS

Latest Lohrmann Blog Posts

mgm

# WAS != "Layer 8"-Security

Example: Pentest / Blackbox-Approach

- pentests are like the search for the needle in the haystack

→ general advantage of attackers

- in contrast: software security as engineering approach

→ methodical approach / delivery of quantifiable results

Make secure (-) — Proof security (+)

role of the security test

# WAS != "Layer 8"-Security

- WAS is not to be understood as a continuation of the classical (IT-) security within the application layer
- WAS is not to be considered as a process to provide more advanced techniques for finding vulnerabilities. The goal must be to avoid the creation of vulnerabilities!
- WAS is software security
  → is secure software development
  → is a software engineering topic
  → is QA (quality assurance)
  → ... and must therefore also fulfill quality procedures.

The key is introducing security into QA processes

# Known examples

# RSA Security

ars TECHNICA SIGN IN

BIZ & IT —

## RSA says hack won't allow "direct attack" ( SecurID tokens

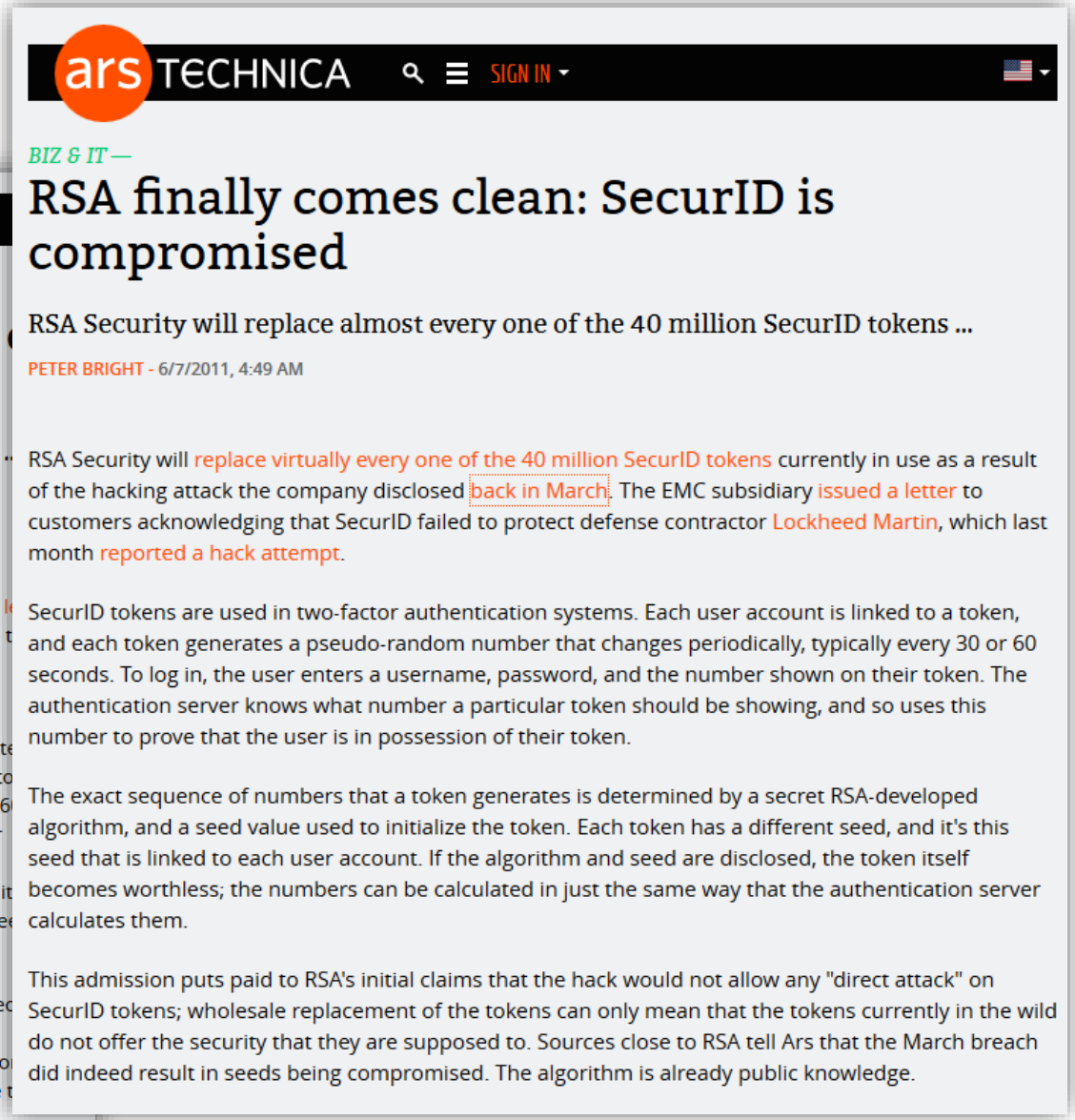
RSA has announced that it was the victim of a hacking operation. Information ...

PETER BRIGHT - 3/19/2011, 9:57 PM

Security firm RSA has been the victim of an "extremely sophisticated" attack that has resulted in exfiltration of certain private information, announced Executive Chairman Art Coviello in an open l published yesterday. The company also filed a note with the SEC, warning of possible risks due to t attack. Since 2006, RSA has been part of EMC.

Some of the information taken relates to the company's SecurID security token hardware and its smartphone-based software equivalent. SecurID tokens are used in two-factor authentication syste to authenticate, users use both a password and a number generated by the SecurID token. Each to generates a sequence of six-digit pseudo-random numbers, with a new number generated every 6 seconds. The number entered by the user must match the number that the authentication server expects the token to generate, and so allows the server to prove that the user not only knows the password, but also is in possession of the token. Each token has a unique 128-bit seed value to init its sequence of numbers. Every user account in the authentication server is associated with the see their respective token; this allows the server to know what random numbers to expect.

RSA's announcement was not specific in the information it gave, so exactly what this means for Sec isn't clear. In the likely worst case, the seed values and their distribution among RSA's 25,000 SecurID-using customers, may have been compromised. This would make it considerably easier fo attackers to compromise systems dependent on SecurID: rather than having to acquire a suitable t they would be required only to eavesdrop on a single authentication attempt (so that they could determine how far through the sequence a particular token was), and from then on would be able to generate numbers at their whim.



ars TECHNICA SIGN IN

BIZ & IT —

## RSA finally comes clean: SecurID is compromised

RSA Security will replace almost every one of the 40 million SecurID tokens ...

PETER BRIGHT - 6/7/2011, 4:49 AM

RSA Security will replace virtually every one of the 40 million SecurID tokens currently in use as a result of the hacking attack the company disclosed back in March. The EMC subsidiary issued a letter to customers acknowledging that SecurID failed to protect defense contractor Lockheed Martin, which last month reported a hack attempt.

SecurID tokens are used in two-factor authentication systems. Each user account is linked to a token, and each token generates a pseudo-random number that changes periodically, typically every 30 or 60 seconds. To log in, the user enters a username, password, and the number shown on their token. The authentication server knows what number a particular token should be showing, and so uses this number to prove that the user is in possession of their token.

The exact sequence of numbers that a token generates is determined by a secret RSA-developed algorithm, and a seed value used to initialize the token. Each token has a different seed, and it's this seed that is linked to each user account. If the algorithm and seed are disclosed, the token itself becomes worthless; the numbers can be calculated in just the same way that the authentication server calculates them.

This admission puts paid to RSA's initial claims that the hack would not allow any "direct attack" on SecurID tokens; wholesale replacement of the tokens can only mean that the tokens currently in the wild do not offer the security that they are supposed to. Sources close to RSA tell Ars that the March breach did indeed result in seeds being compromised. The algorithm is already public knowledge.

# DigiNotar

ars TECHNICA SIGN IN

BIZ & IT —

## Another fraudulent cert… same old questions abou… authorities

For the second time this year, Iranian hackers…

PETER BRIGHT - 8/30/2011, 5:12 AM

Earlier this year, an Iranian hacker broke into servers bel… Comodo and issued himself a range of certificates for sit… With these certificates, he could eavesdrop on users of th… protect their mail sessions.

It's happened again. This time, Dutch certificate authority… for google.com and all subdomains. As before, Gmail app… appears to be Iranian, with reports that the certificate ha… attacks in that country. The certificate was issued on July… weeks prior to its discovery.

DigiNotar has revoked the certificate, which provides son… applications do not bother checking for revocations). How… how the certificate was issued in the first place, making it… a result, Google and Mozilla have both made patches to … the entire certificate authority.

COMPUTERWORLD FROM IDG

## One year after DigiNotar breach, Fox… extent of compromise

The hacker gained admin access to all critical DigiN… authority systems despite network segmentation, …

By Lucian Constantin

Romania Correspondent, IDG News Service | OCT 31, 2012 7:07 PM PT

The 2011 security breach at Dutch certificate authority (C… resulted in an extensive compromise and was facilitated … shortcomings in the company's network segmentation a… configuration, according to Fox-IT, the security company… the Dutch government to investigate the incident.

"The DigiNotar network was divided into 24 different inte… segments," Fox-IT said in its final investigation report, pu… this week by the Dutch Ministry of Interior and Kingdom … internal and external Demilitarized Zone (DMZ) separated … of the internal network from the Internet. The zones wer… described or enforced and the firewall contained many r… exceptions for network traffic between the various segm…

The DigiNotar security breach occurred in July 2011 and … hacker using the company's certificate authority (CA) infr… issue hundreds of rogue digital certificates for high-profi… including one for google.com that was later used in a ma… attack against Internet users in Iran. After the incident be… browser and operating system developers revoked their …

NETWORKWORLD FROM IDG INSIDER Sign In | Register

## DigiNotar certificate authority goes bankrupt

Victim of theft of 500-plus SSL certificates, Dutch company couldn't survive

By Tim Greene

Executive Editor, Network World | SEP 20, 2011 1:24 PM PT

The theft of SSL certificates from Dutch certificate authority DigiNotar so undermined trust in the company that it has gone bankrupt.

Responsible for taking down the company is a single attacker, believed to be in Iran, who stole more than 500 certificates used to authenticate sites that make secure connections via SSL. DigiNotar was the primary certificate authority used by the Dutch government.

DigiNotar filed for bankruptcy yesterday and a Dutch court approved the filing today. Trustees were appointed to liquidate its assets, according to a statement by DigiNotar's parent company, Vasco.

**MORE ON SECURITY CERTIFICATES:** Former cybersecurity czar Clarke says smartphones, digital certificates create huge security problems

The industry has been running from DigiNotar since the breach was made public Aug. 29, more than two months after the company discovered an attack. Microsoft has blacklisted all DigiNotar digital certificates, deeming them untrusted. Google and Mozilla had already blacklisted the company's certificates, and the TOR project has recommended rejecting all DigiNotar certificates.

mgm

# Bank Robbery in the 21st century

- Criminals buy zombie pcs on the black market
  - Especially those that have an IP in the bank sector
- Install targeted malware on these zombie pcs
  - (again bought on the black market)
- Compromise as many more machines in the network as possible
  - Special focus on mail servers!!!
  - (to make sure the attack was not detected)
  - (and to perform targeted spear-phishing attacks)
- Via admin accounts: access to separated ATM network segment
  - Manipulate the ATMs to give out more money
- ~42 days from first infection to robbery
- Affected ATMs: Wincor Nixdorf

mgm

KrebsonSecurity
In-depth security news and investigation

## 22 Gang Hacked ATMs from Inside Banks

DEC 14

An organized gang of hackers from Russia and Ukraine has broken into internal networks at dozens of financial institutions and installed malicious software that allowed the gang to drain bank ATMs of cash. While none of the victim institutions were in the United States or Western Europe, experts say the stealthy methods used by the attackers in these heists would likely work across a broad range of western banks.

Most cybercrime targets consumers and businesses, stealing account information such as passwords and other data that lets thieves cash out hijacked bank accounts, as well as credit and debit cards. But this gang specializes in hacking into banks directly, and then working out ingenious ways to funnel cash directly from the financial institution itself.

A number of the gang's members are believed to be tied to a group of Eastern European hackers accused of stealing more than USD $2 million from Russian banks using a powerful, custom-made banking trojan known as Carberp. Eight men in Moscow were arrested in 2012 and accused of building and using Carberp, but sources say the core members of the gang were out of jail within hours after their arrest and have been busy rebuilding their crime machine ever since.

According to report released today by Fox-IT and Group-IB, security firms based in The Netherlands and Russia, respectively, the Carberp guys have since changed their tactics: Instead of stealing from thousands of bank account holders, this gang has decided to focus on siphoning funds right out of banks' coffers. So far, the security firms report, the gang has stolen more than $15 million from Eastern European banks.

# Blackmailing of german webhoster 1blu

- Blackmailer wants 250,000 EUR in exchange for not publishing user data
  - Bank accounts, passwords, other personal data
  - Money to be payed in bitcoins
- 1blu does not pay, informs police and resets all user passwords
- Two months later: reveal that also SSL certificates of customers have been compromised

heise Security News Hintergrund Tools Foren

Security > News > 7-Tage-News > 2015 > KW 33 > Webhoster 1blu gehackt und erpresst

« Vorige | Nächste »

**Webhoster 1blu gehackt und erpresst**

13.08.2015 09:38 Uhr – Ronald Eikenberg vorlesen

1blu

**Ein Online-Erpresser hat sich weitreichenden Zugriff auf die Infrastruktur von 1blu verschafft – darunter Passwörter und Bankverbindungen sämtlicher Kunden. Um die Veröffentlichung zu verhindern, sollte der Hoster 250.000 Euro zahlen.**

Die Webhosting-Firma 1blu ist Opfer eines Cyber-Erpressers geworden. Ein bislang unbekannter Täter ist in die Infrastruktur des Unternehmens eingedrungen und konnte dabei unter anderem auf die Daten sämtlicher Kunden zugreifen.

Betroffen sind unter anderem die bei 1blu gespeicherten Passwörter, persönliche Daten, Bankverbindungen und Interna. Anschließend versuchte er das Unternehmen zur Zahlung von umgerechnet 250.000 Euro in Bitcoins zu erpressen, wie das Unternehmen im Gespräch mit heise Security erklärte. Andernfalls wolle er die erbeuteten Daten veröffentlichen.

mgm

# Ransomware

Los Angeles Times

SUBSCRIBE

LOCAL ENTERTAINMENT SPORTS POLITICS OPINION MOST POPULAR PLACE AN AD

MONDAY
OCT. 30, 2017

## Hollywood hospital pays $17,000 in bitcoin to hackers; FBI investigating

FEBRUARY 18, 2016, 10:44 AM

Hollywood Presbyterian Medical Center paid a $17,000 ransom in bitcoin to a hacker who seized control of the hospital's computer systems and would give back access only when the money was paid, the hospital's chief executive said Wednesday.

The assault on Hollywood Presbyterian occurred Feb. 5, when hackers using malware infected the institution's computers, preventing hospital staff from being able to communicate from those devices, said Chief Executive Allen Stefanek.

The hacker demanded 40 bitcoin, the equivalent of about $17,000, he said.

**Join the conversation on Facebook >>**

"The malware locks systems by encrypting files and demanding ransom to obtain the decryption key. The quickest and most efficient way to restore our systems and administrative functions was to pay the ransom and obtain the decryption key," Stefanek said. "In the best interest of restoring normal operations, we did this."

The hospital said it alerted authorities and was able to regain control of all its computer systems by Monday, with the assistance of technology experts.

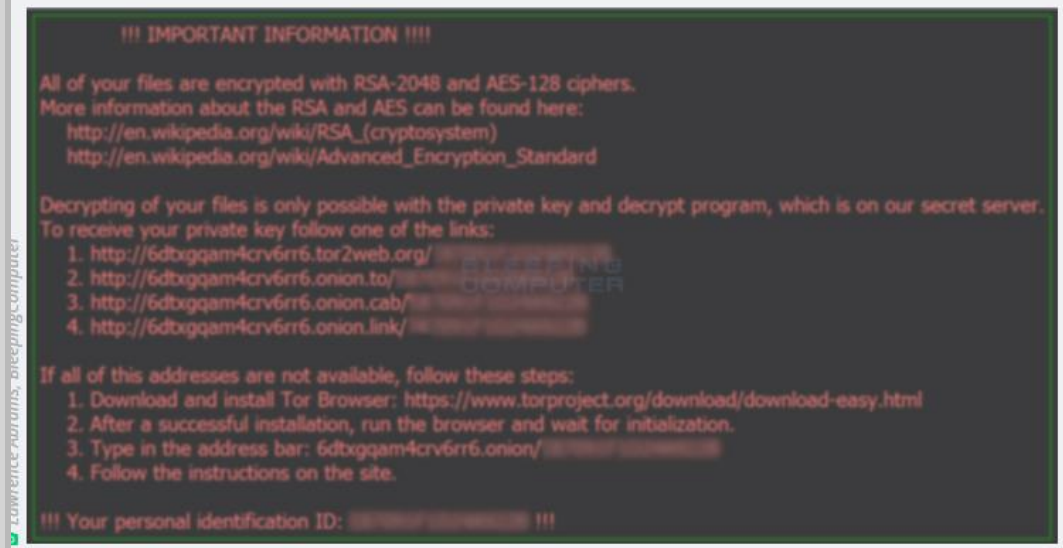
ars TECHNICA SIGN IN

*PLEASE LET ME INFECT YOU —*

## "Locky" crypto-ransomware rides in on malicious Word document macro

Malware depends on users falling for its pleas—twice if Office macros aren't on.

SEAN GALLAGHER - 2/17/2016, 11:36 PM




Several security researchers have discovered a new type of malware that jumps onto the ransomware bandwagon, encrypting victims' files and then demanding a payment of half a bitcoin for the key. Named "Locky," the malware depends on a rather low-tech installation method to take root in a user's system: it arrives courtesy of a malicious macro in a Word document.

Security researchers Kevin Beaumont and Lawrence Abrams each wrote an analysis of Locky on Tuesday, detailing how it installs itself and its components. The carrier document arrives in an e-mail that claims to be delivering an invoice (with a subject line that includes an apparently random invoice number starting with the letter J). When the document is opened, if Office macros are turned on in Word, then the malware installation begins. If not, the victim sees blocks of garbled text in the Word

# Data loss / data breach

- Hospitals are often popular targets for attacker
  - insufficient security
  - lots of sensitive data

Chicago Tribune

SUBSCRIBE

SPORTS BREAKING MOST POPULAR OPINION SUBURBS ENTERTAINMENT BUSINESS ADVERTISING 45°

## Advocate to pay $5.5 million over data breach: record HIPAA settlement

By **Lisa Schencker** · **Contact Reporter**
Chicago Tribune

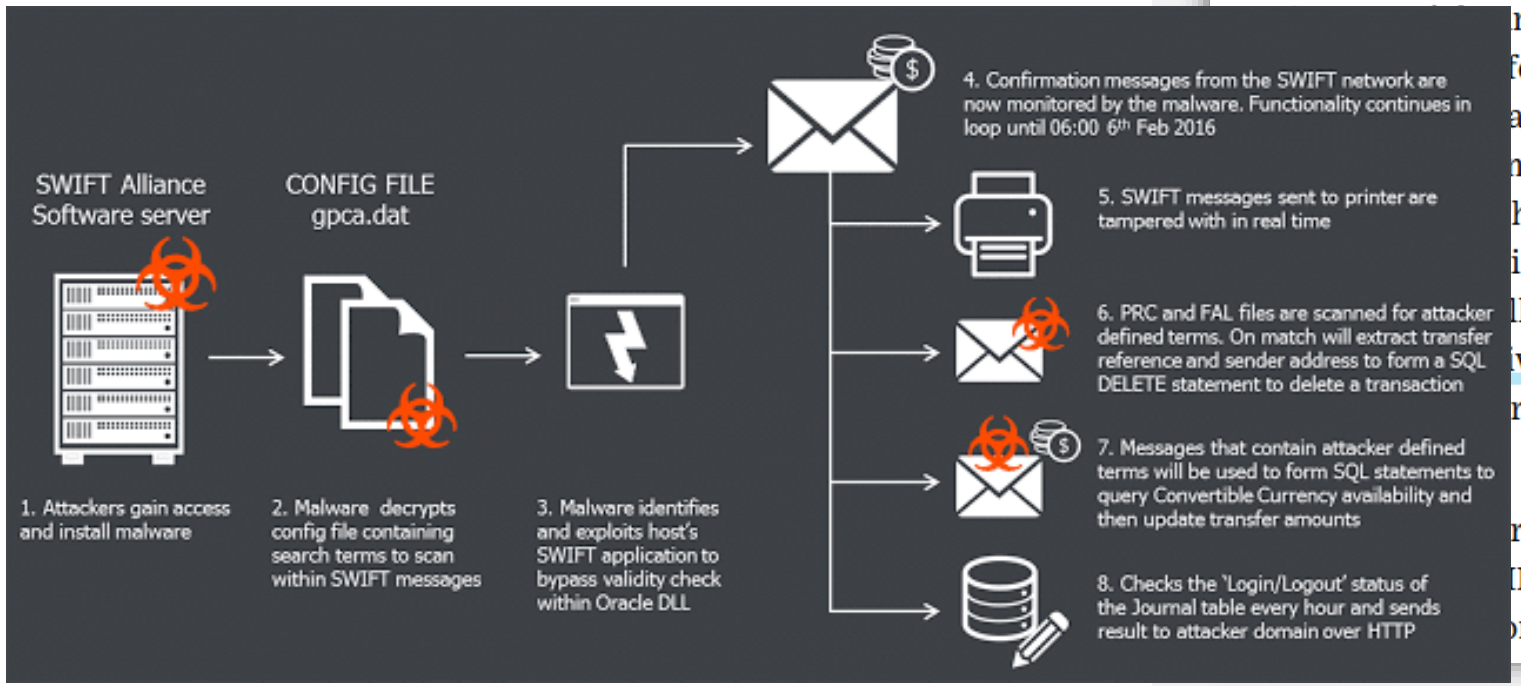
AUGUST 5, 2016, 7:20 AM

Advocate Health Care will pay $5.55 million to settle allegations it violated federal patient privacy law — the largest such settlement paid by a single entity.

The settlement with the federal government follows an investigation that began in 2013 when Advocate reported three separate data breaches involving its physician-led medical group subsidiary, Advocate Medical Group. The breaches involved the electronic health information of 4 million people, including medical information, names, credit card numbers and birthdays, among other things.

# Central bank of Bangladesh heist

- Attackers steal 81 million USD
- Hack of the banks SWIFT systems
  - abused to make malicious transactions
- Money laundered via Philippines' banks




**That Insane, $81M Bangladesh Bank Heist? Here's What We Know**

## What Happened?

On February 4, unknown hackers used SWIFT credentials of Bangladesh Central Bank employees to send more than three dozen fraudulent money transfer requests to the Federal Reserve Bank of New York asking the bank to transfer millions of the Bangladesh Bank's funds to bank accounts in the Philippines, Sri Lanka and other parts of Asia.

The hackers managed to get $81 million sent to Rizal
nking Corporation in the Philippines via four
fer requests and an additional $20 million
a Banking in a single request. But the
nk managed to halt $850 million in other
he $81 million was deposited into four
izal branch in Manila on Feb. 4. These
ll been opened a year earlier in May 2015, but
ive with just $500 sitting in them until the
rived in February this year, according to

r" helped Bangladesh Bank discover the heist.
FT system is configured to automatically
rd each time a money transfer request goes

More details on: http://baesystemsai.blogspot.de/2016/04/two-bytes-to-951m.html

mgm

# Telecom company TalkTalk hacked

- Customer data stolen
  - blackmail attempts
  - TalkTalk informs its customers
- Later:
  - phishing attacks etc. against customers

- What is the cost of such an attack?

WIRED

Security

## TalkTalk fined £400,000 after 150,000 customer details were stolen in 2015

The Information Commissioner's Office issued the fine after it found it was easy for hackers

## Boy, 17, admits TalkTalk hacking offences

15 November 2016 | Norfolk

Share

**A 17-year-old boy has admitted hacking offences linked to a data breach at the communications firm TalkTalk, claiming he was "just showing off" to friends.**

Norwich Youth Court was told he had used hacking tool software to identify vulnerabilities on target websites.

The data haul netted email addresses, names and phone numbers, as well as 21,000 unique bank account numbers and sort codes.

The boy pleaded guilty to seven charges and will be sentenced next month.

The technique used by the attacker, called SQL injection, has been well known in security circles for almost 20 years. "SQL injection is well understood, defences exist and TalkTalk ought to have known it posed a risk to its data," the ICO said. "On top of that the company also had two early warnings that it was unaware of. The first was same vulner 3 September

The attack was branded a "car crash" by former information commission Christopher Graham.

The company claimed the hack cost the firm £42m but has since reported a surge in half-year profits.

It said it also lost 98,000 broadband customers in the first half of the year, though this was largely offset by 69,000 new customers signing up.

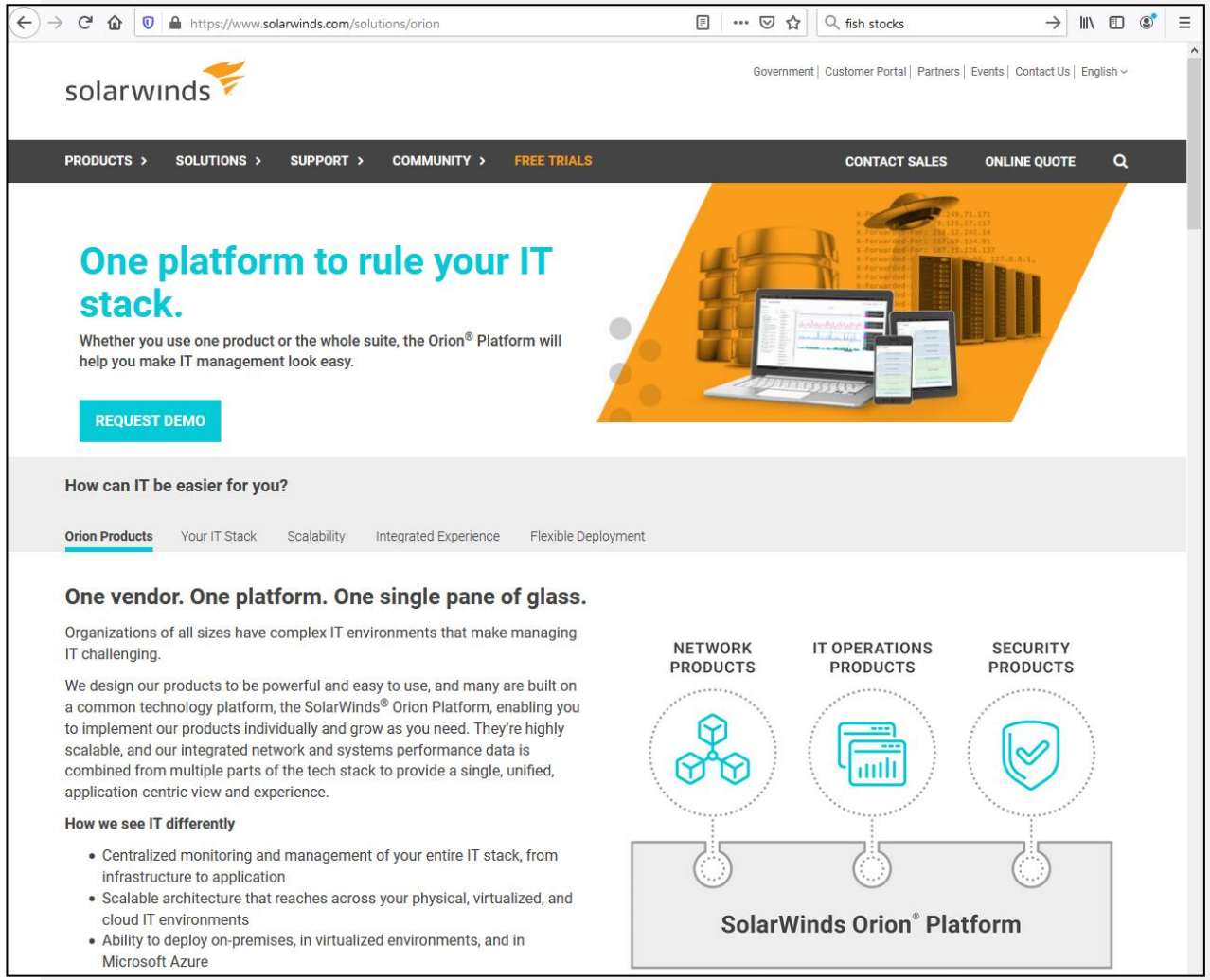
th Denham, the Information Commissioner, said TalkTalk "should have ore" to protect customer information and that it failed to "implement the sic cyber security measures."

mgm

# SolarWinds Sunburst

## Supply Chain Attack

- 300.000 customers; ~18.000 affected
  - (i.a. FireEye, VMware, multiple US government agencies, ...)
- Update Server were compromised (March '20)
  - Weak password (solarwinds123), access publicly available on github
  - Malware inside the updates of the Orion Platform (Monitoring & Management Solution) → correctly signed
- A lot of attack diffusion measures (attack discovery in December '20)
  - Long retention period before C&C connection (12 to 14 days)
  - Highly customized attacks (GEO-IP addresses, DNS names)
  - new malware? (nearly no code overlap to known ones)

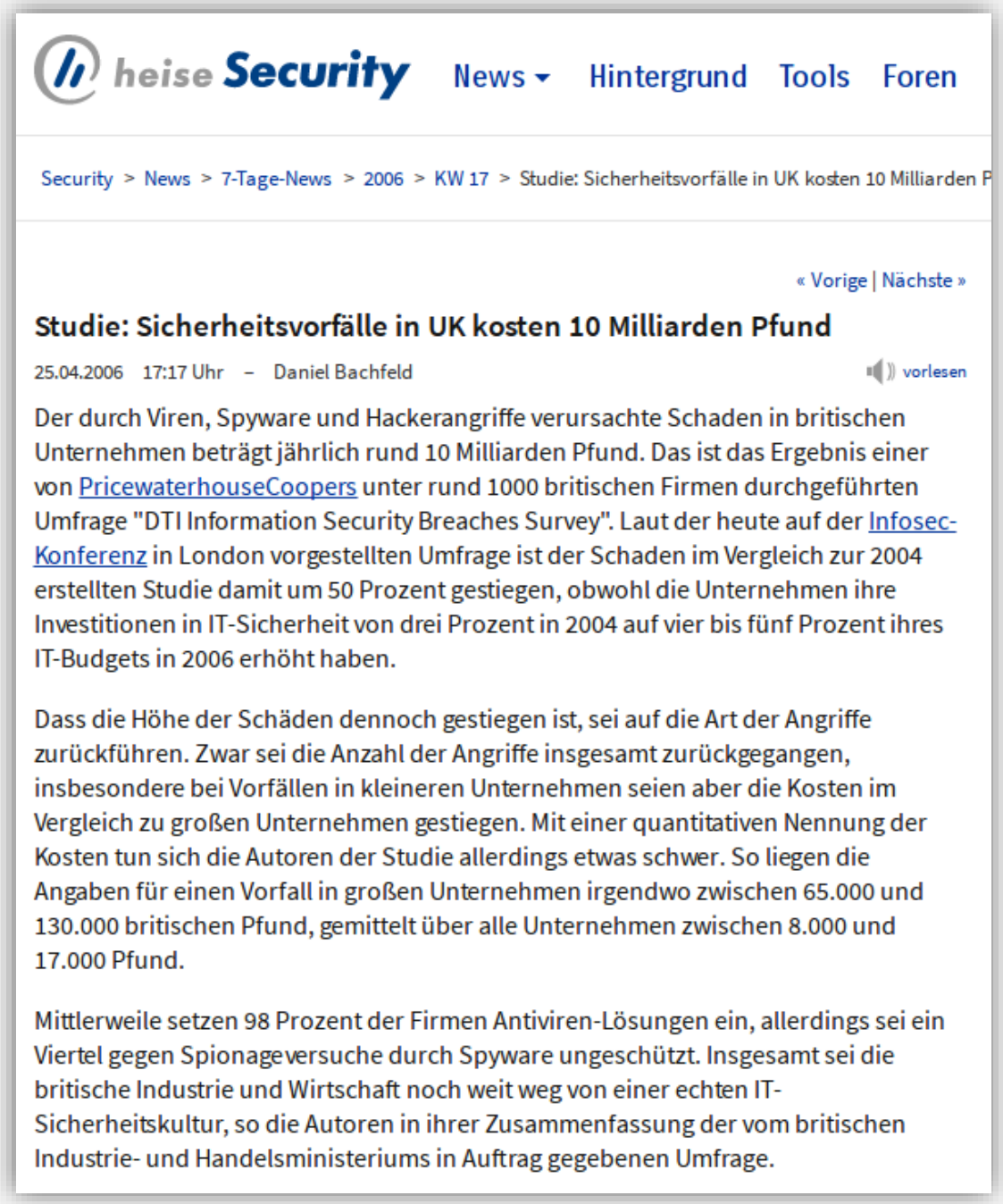



mgm

# Studies

# Security Incidents UK

- Estimated costs:
  - 65.000 – 130.000 pounds per incident



heise Security News Hintergrund Tools Foren

Security > News > 7-Tage-News > 2006 > KW 17 > Studie: Sicherheitsvorfälle in UK kosten 10 Milliarden P

« Vorige | Nächste »

**Studie: Sicherheitsvorfälle in UK kosten 10 Milliarden Pfund**

25.04.2006 17:17 Uhr – Daniel Bachfeld vorlesen

Der durch Viren, Spyware und Hackerangriffe verursachte Schaden in britischen Unternehmen beträgt jährlich rund 10 Milliarden Pfund. Das ist das Ergebnis einer von PricewaterhouseCoopers unter rund 1000 britischen Firmen durchgeführten Umfrage "DTI Information Security Breaches Survey". Laut der heute auf der Infosec-Konferenz in London vorgestellten Umfrage ist der Schaden im Vergleich zur 2004 erstellten Studie damit um 50 Prozent gestiegen, obwohl die Unternehmen ihre Investitionen in IT-Sicherheit von drei Prozent in 2004 auf vier bis fünf Prozent ihres IT-Budgets in 2006 erhöht haben.

Dass die Höhe der Schäden dennoch gestiegen ist, sei auf die Art der Angriffe zurückführen. Zwar sei die Anzahl der Angriffe insgesamt zurückgegangen, insbesondere bei Vorfällen in kleineren Unternehmen seien aber die Kosten im Vergleich zu großen Unternehmen gestiegen. Mit einer quantitativen Nennung der Kosten tun sich die Autoren der Studie allerdings etwas schwer. So liegen die Angaben für einen Vorfall in großen Unternehmen irgendwo zwischen 65.000 und 130.000 britischen Pfund, gemittelt über alle Unternehmen zwischen 8.000 und 17.000 Pfund.

Mittlerweile setzen 98 Prozent der Firmen Antiviren-Lösungen ein, allerdings sei ein Viertel gegen Spionageversuche durch Spyware ungeschützt. Insgesamt sei die britische Industrie und Wirtschaft noch weit weg von einer echten IT-Sicherheitskultur, so die Autoren in ihrer Zusammenfassung der vom britischen Industrie- und Handelsministeriums in Auftrag gegebenen Umfrage.

# Costs of identity theft

heise Security News Hintergrund Tools Foren

Security > News > 7-Tage-News > 2012 > KW 41 > Studie: Cybercrime verursacht deutschen Unternehme

« Vorige | Nächste »

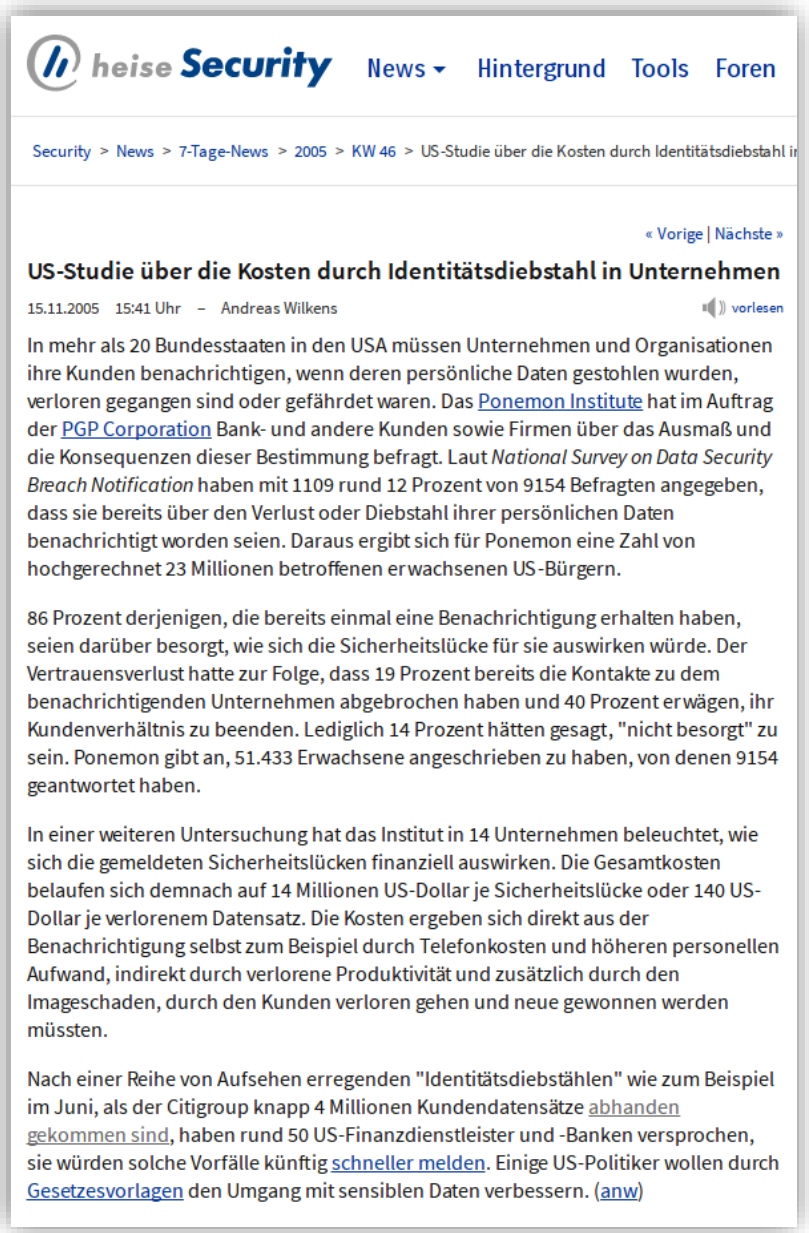
**Studie: Cybercrime verursacht deutschen Unternehmen Millionenschäden**

08.10.2012 18:05 Uhr vorlesen

Datendiebstahl, Computerviren und Web-Attacken verursachen in einem deutschen Großunternehmen laut einer Studie von Hewlett-Packard jährlich einen Schaden von durchschnittlich 4,8 Millionen Euro. Deutschland liegt damit zwischen den USA (6,9 Millionen Euro) und Japan (3,9 Millionen Euro), wie das IT-Unternehmen am Montag in Böblingen bei Stuttgart mitteilte.

Pro Woche gibt es in den für die Studie untersuchten Unternehmen und Behörden 1,1 erfolgreiche Angriffe – verglichen mit 1,8 in den USA. Allein 40 Prozent des geschätzten Schadens entfallen auf Datenverluste – oft verursacht durch "Taten krimineller Insider". Weitere 28 Prozent fallen als Umsatzeinbußen an, etwa wenn nach einer Denial-of-Service-Attacke die Shopping-Webseite lahmgelegt wird.

Für die HP-Studie "Cost of Cyber Crime" befragte das Ponemon Institute 418 Fach- und Führungskräfte aus 43 Unternehmen sowie Behörden mit 1044 bis 95.412 Computer-Arbeitsplätzen. Für Deutschland wurde die Erhebung in diesem Rahmen zum ersten Mal vorgenommen. In den USA stellte HP fest, dass sich die Zahl der Angriffe in den vergangenen drei Jahren mehr als verdoppelt hat. Die Kosten stiegen dadurch um rund 40 Prozent. (*dpa*) / (axk)



heise Security News Hintergrund Tools Foren

Security > News > 7-Tage-News > 2005 > KW 46 > US-Studie über die Kosten durch Identitätsdiebstahl i

« Vorige | Nächste »

**US-Studie über die Kosten durch Identitätsdiebstahl in Unternehmen**

15.11.2005 15:41 Uhr – Andreas Wilkens vorlesen

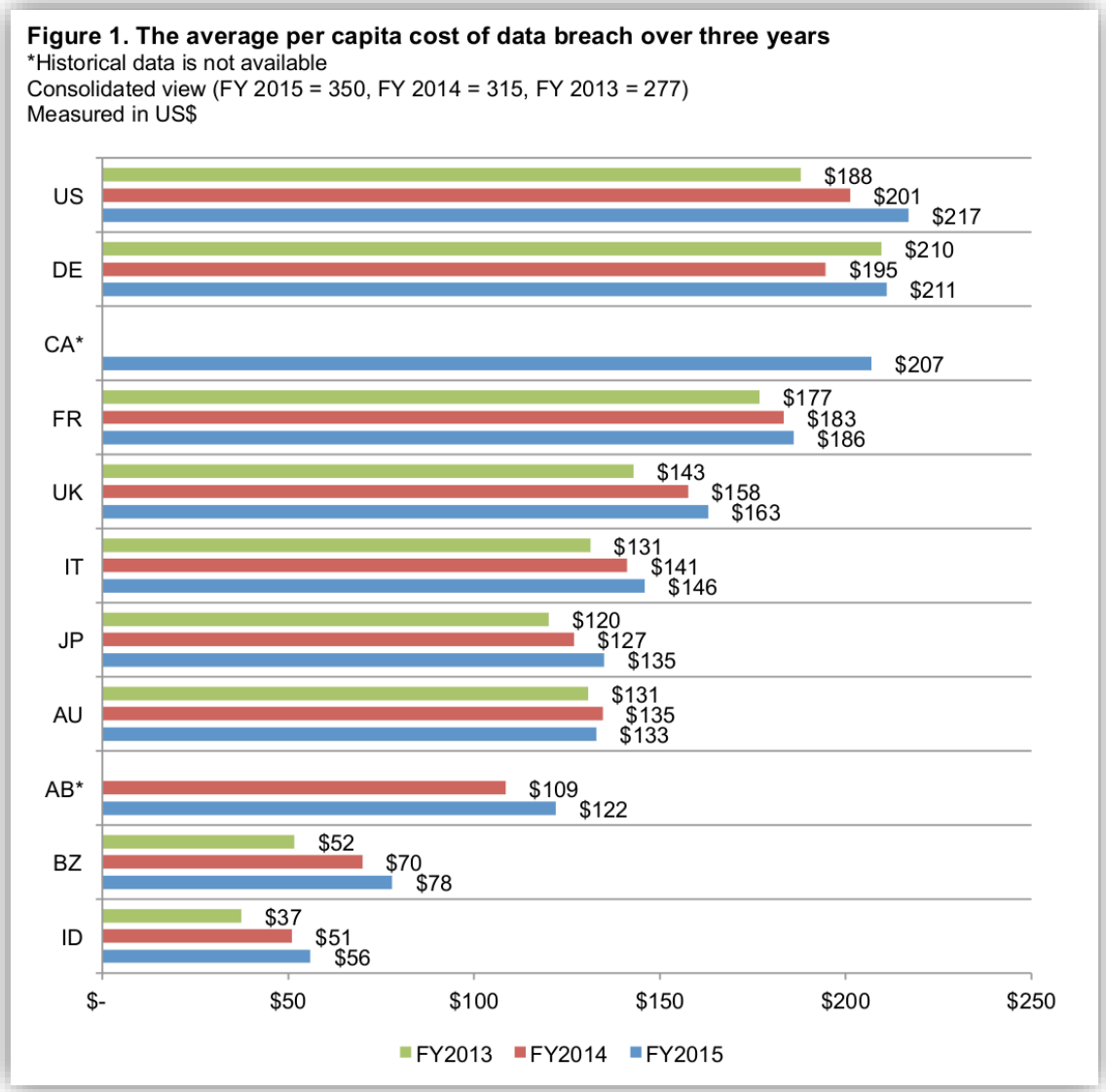
In mehr als 20 Bundesstaaten in den USA müssen Unternehmen und Organisationen ihre Kunden benachrichtigen, wenn deren persönliche Daten gestohlen wurden, verloren gegangen sind oder gefährdet waren. Das Ponemon Institute hat im Auftrag der PGP Corporation Bank- und andere Kunden sowie Firmen über das Ausmaß und die Konsequenzen dieser Bestimmung befragt. Laut *National Survey on Data Security Breach Notification* haben mit 1109 rund 12 Prozent von 9154 Befragten angegeben, dass sie bereits über den Verlust oder Diebstahl ihrer persönlichen Daten benachrichtigt worden seien. Daraus ergibt sich für Ponemon eine Zahl von hochgerechnet 23 Millionen betroffenen erwachsenen US-Bürgern.

86 Prozent derjenigen, die bereits einmal eine Benachrichtigung erhalten haben, seien darüber besorgt, wie sich die Sicherheitslücke für sie auswirken würde. Der Vertrauensverlust hatte zur Folge, dass 19 Prozent bereits die Kontakte zu dem benachrichtigenden Unternehmen abgebrochen haben und 40 Prozent erwägen, ihr Kundenverhältnis zu beenden. Lediglich 14 Prozent hätten gesagt, "nicht besorgt" zu sein. Ponemon gibt an, 51.433 Erwachsene angeschrieben zu haben, von denen 9154 geantwortet haben.

In einer weiteren Untersuchung hat das Institut in 14 Unternehmen beleuchtet, wie sich die gemeldeten Sicherheitslücken finanziell auswirken. Die Gesamtkosten belaufen sich demnach auf 14 Millionen US-Dollar je Sicherheitslücke oder 140 US-Dollar je verlorenem Datensatz. Die Kosten ergeben sich direkt aus der Benachrichtigung selbst zum Beispiel durch Telefonkosten und höheren personellen Aufwand, indirekt durch verlorene Produktivität und zusätzlich durch den Imageschaden, durch den Kunden verloren gehen und neue gewonnen werden müssten.

Nach einer Reihe von Aufsehen erregenden "Identitätsdiebstählen" wie zum Beispiel im Juni, als der Citigroup knapp 4 Millionen Kundendatensätze abhanden gekommen sind, haben rund 50 US-Finanzdienstleister und -Banken versprochen, sie würden solche Vorfälle künftig schneller melden. Einige US-Politiker wollen durch Gesetzesvorlagen den Umgang mit sensiblen Daten verbessern. (anw)

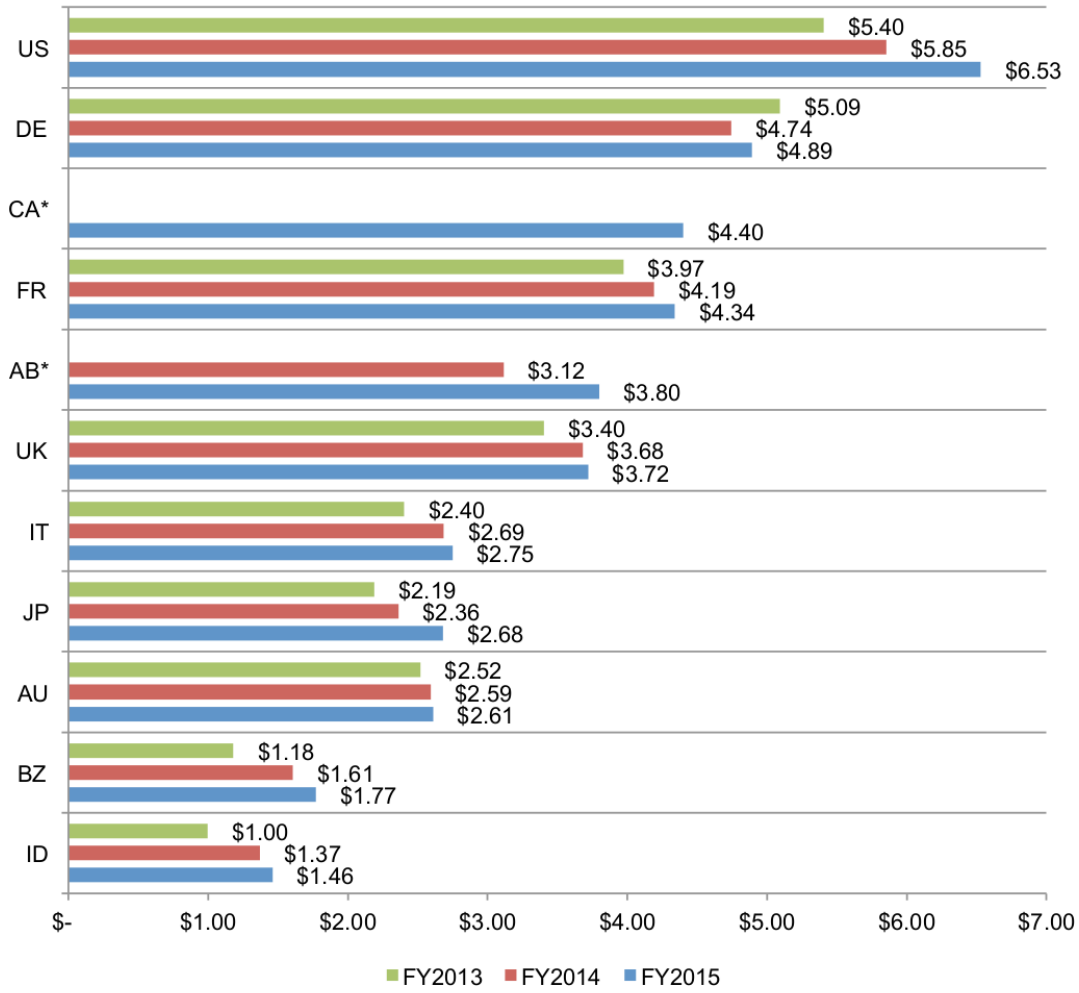
# Average cost of an incident




(costs per customer data set)

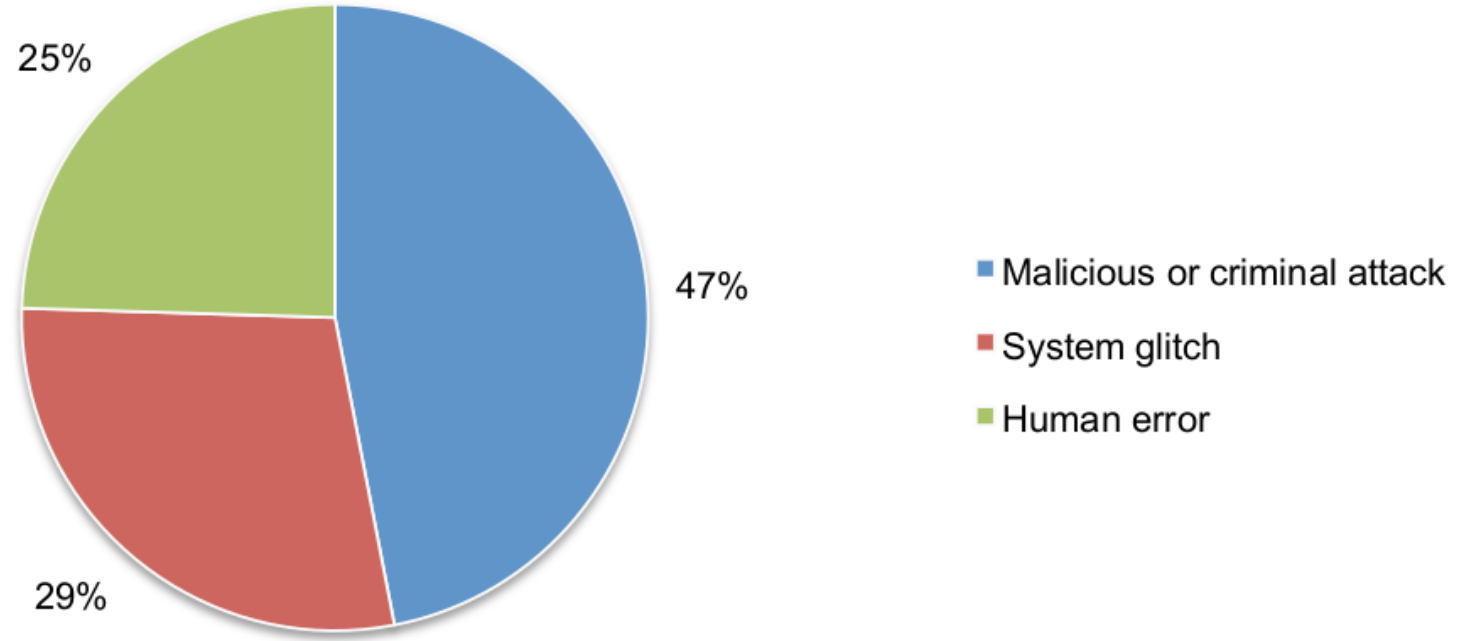
# Average total cost of an incident

**Figure 2. The average total organizational cost of a data breach over three years**
*Historical data is not available
Consolidated view (FY 2015 = 350, FY 2014 = 315, FY 2013 = 277)
Measured in US$ (millions)

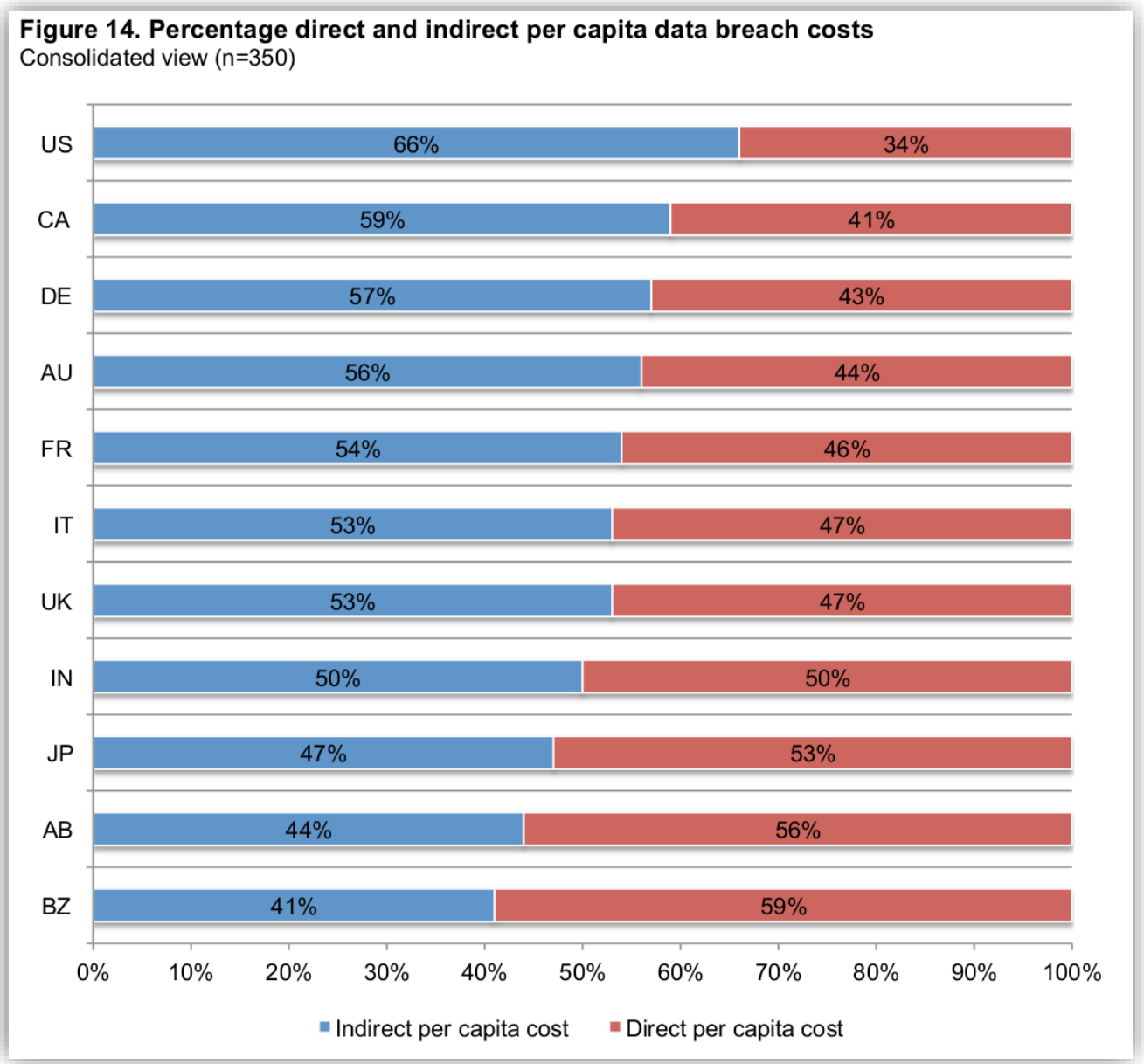


# Root cause

**Pie Chart 2. Distribution of the benchmark sample by root cause of the data breach**
Consolidated view (n=350)

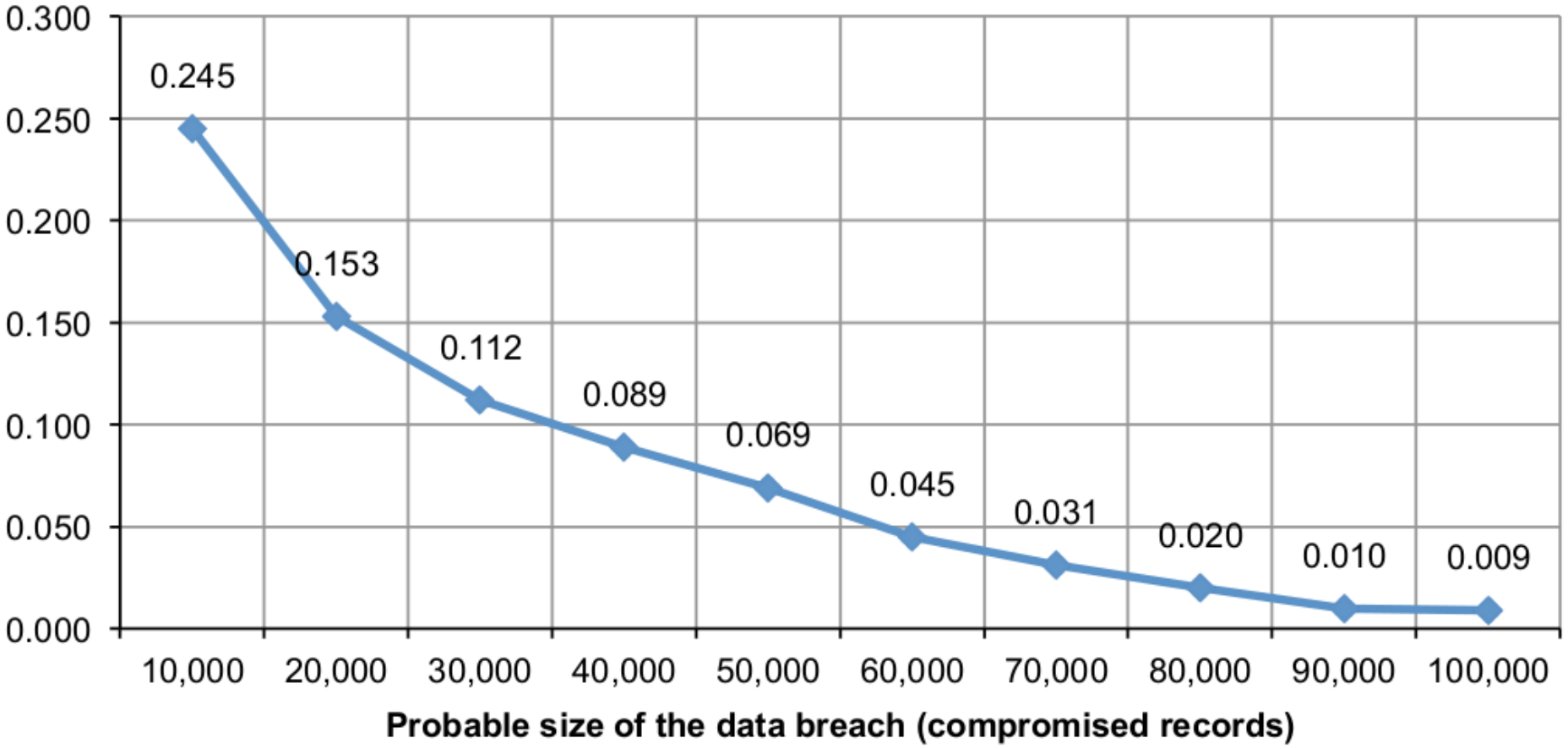


# Indirect costs



# Probability of occurrence

**Figure 15. Probability of a data breach involving a minimum of 10,000 to 100,000 records**
Consolidated view (n=350)



# Basic Terms

# Differentiation: Safety vs. Security

„Sicherheit“
(german)

“Safety”


Photo by Cathal Mac an Bheatha on Unsplash

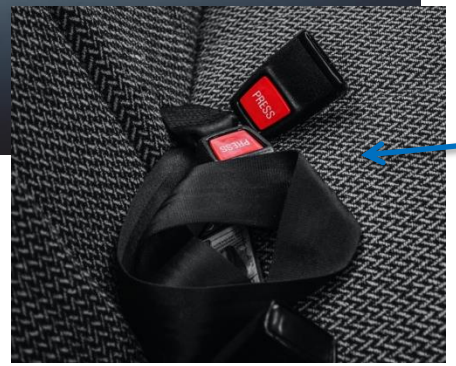



Photo by Therese Mikkelsen Skaar on Unsplash

safety belt

“Security”

security belt

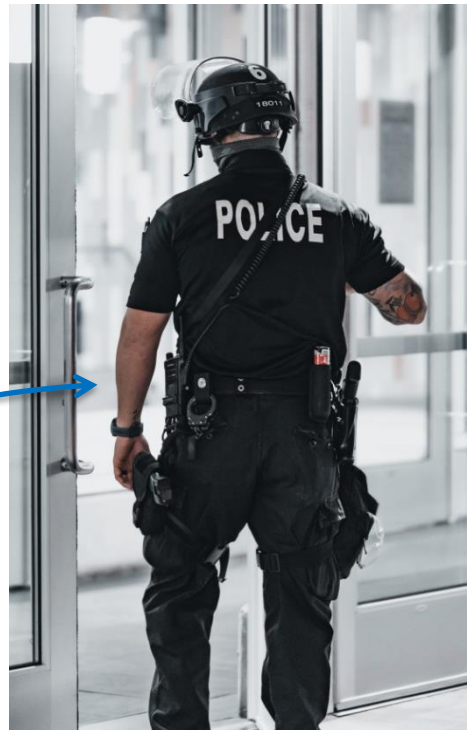


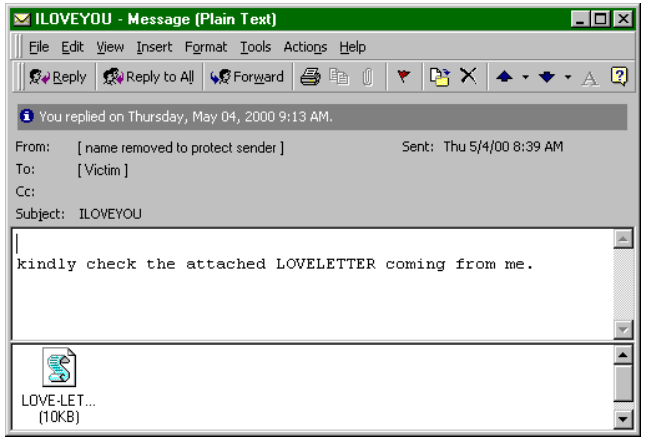

Photo by LOGAN WEAVER on Unsplash

# Malware (**mal**icious soft**ware)**

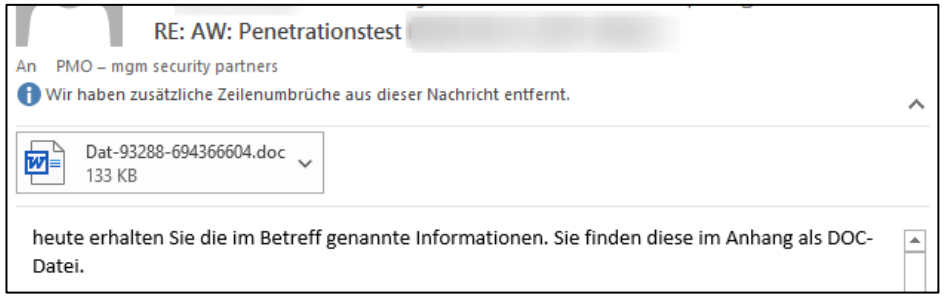
2 ways of infection

Exploitation of a vulnerability
- drive-by-download
- Direct exploitation

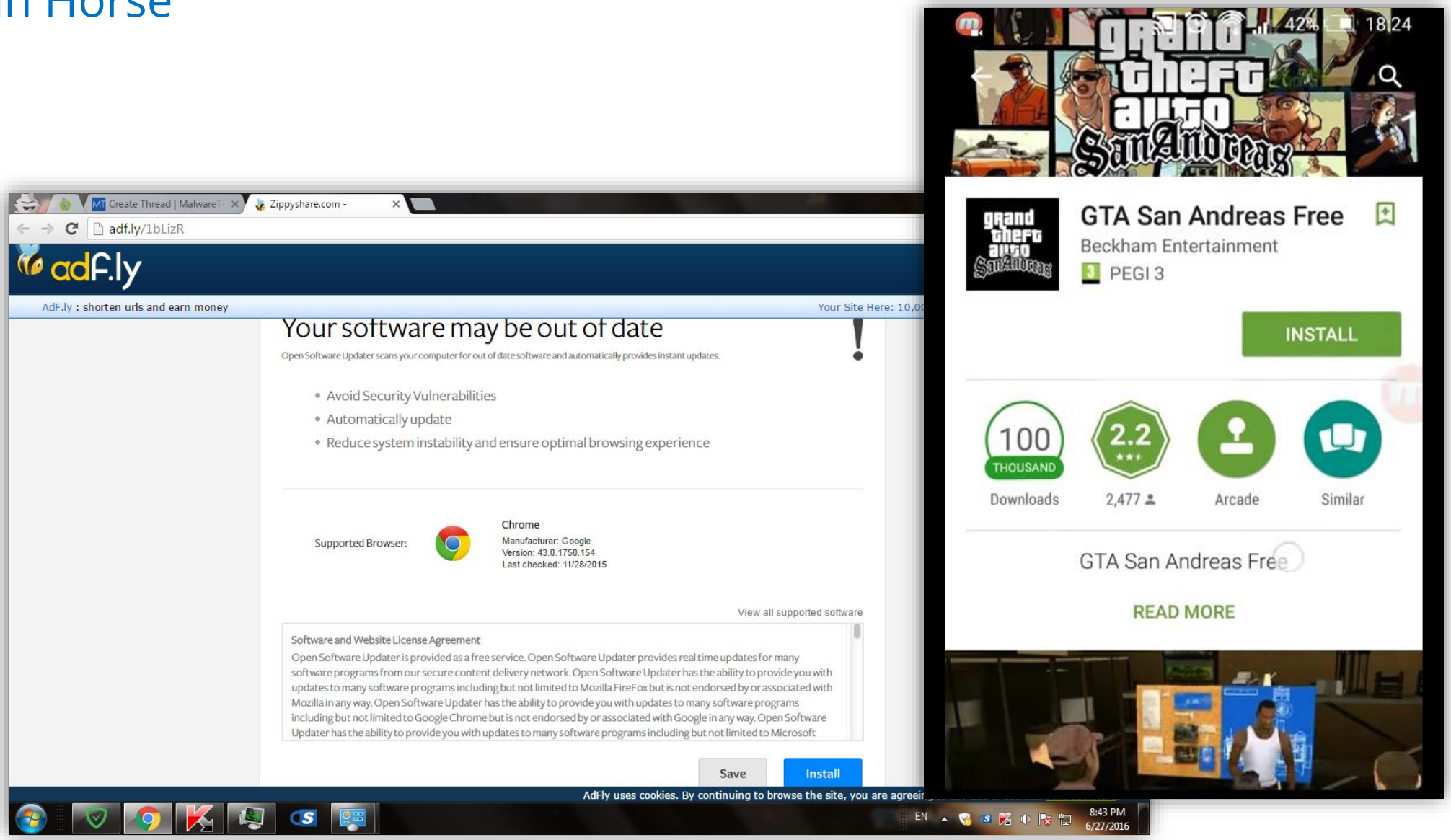
Included in a file
- Trojan Horse



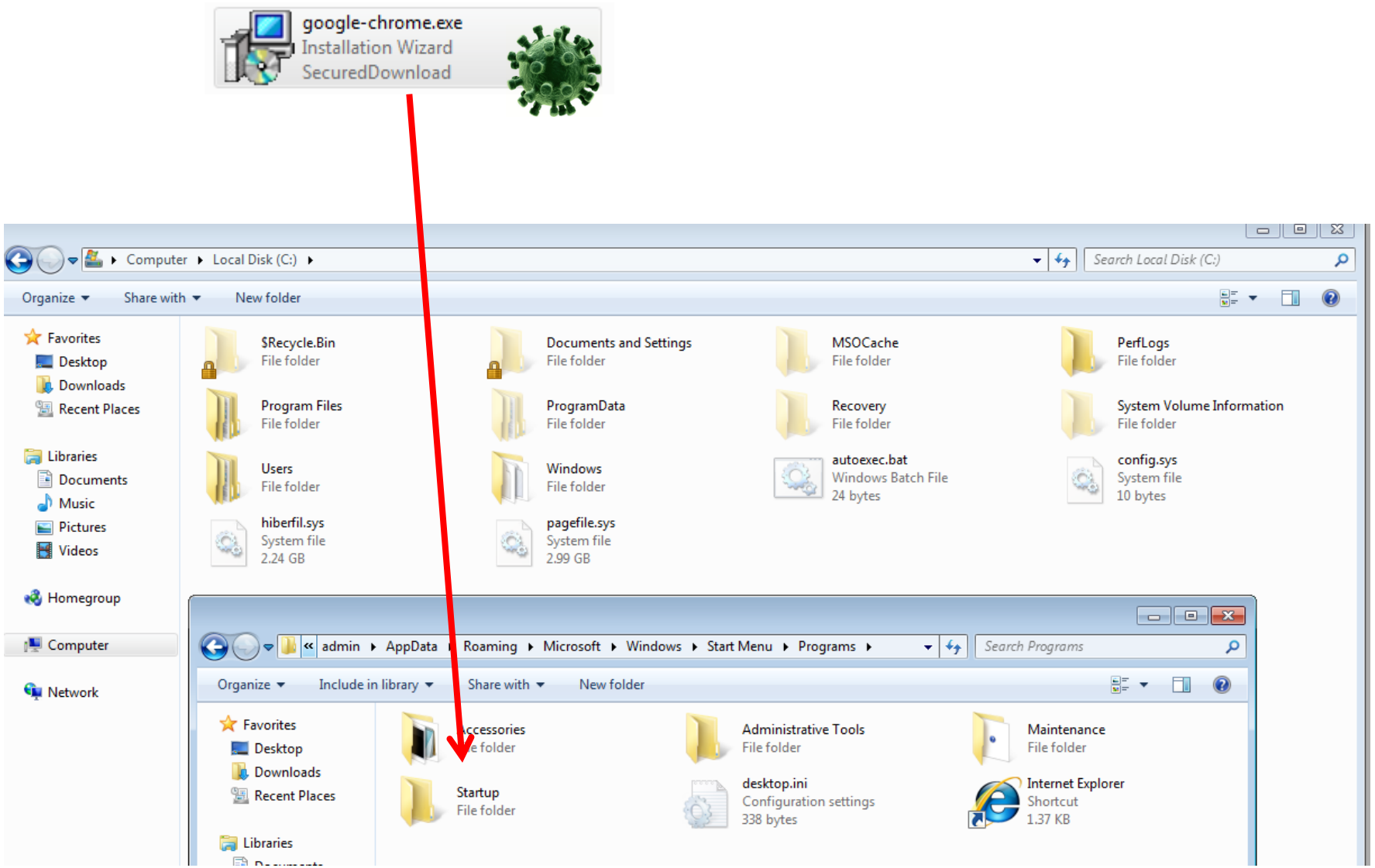




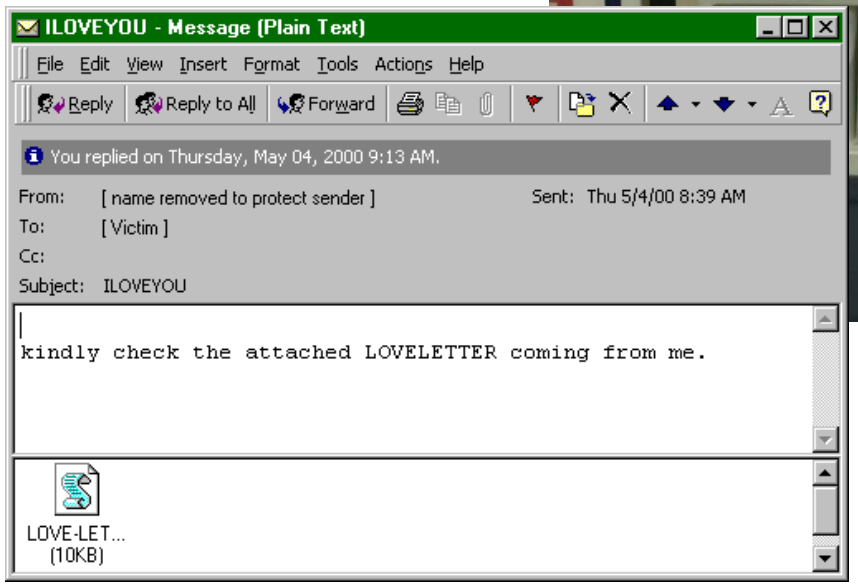
# Trojan Horse



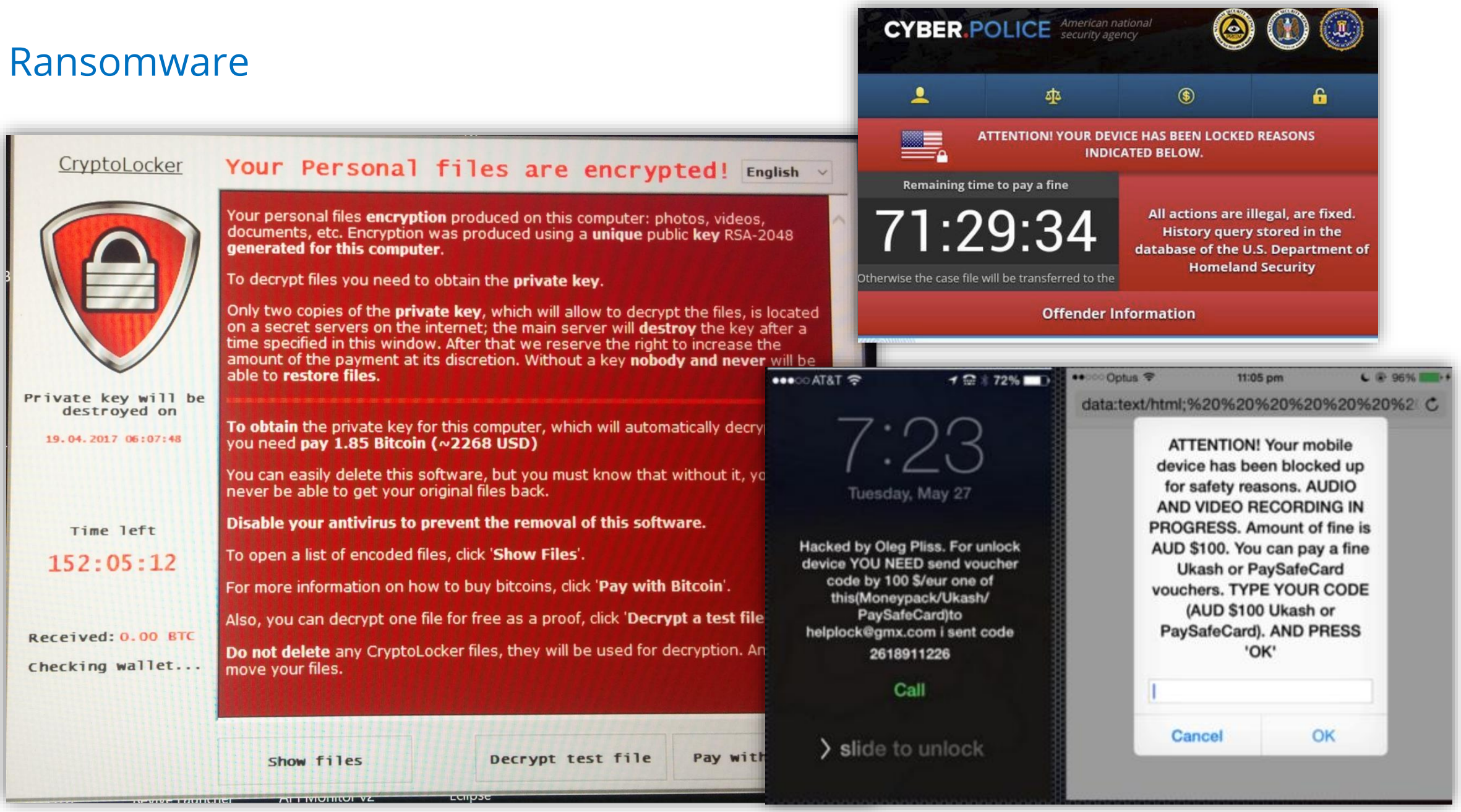
# Virus



# Worm

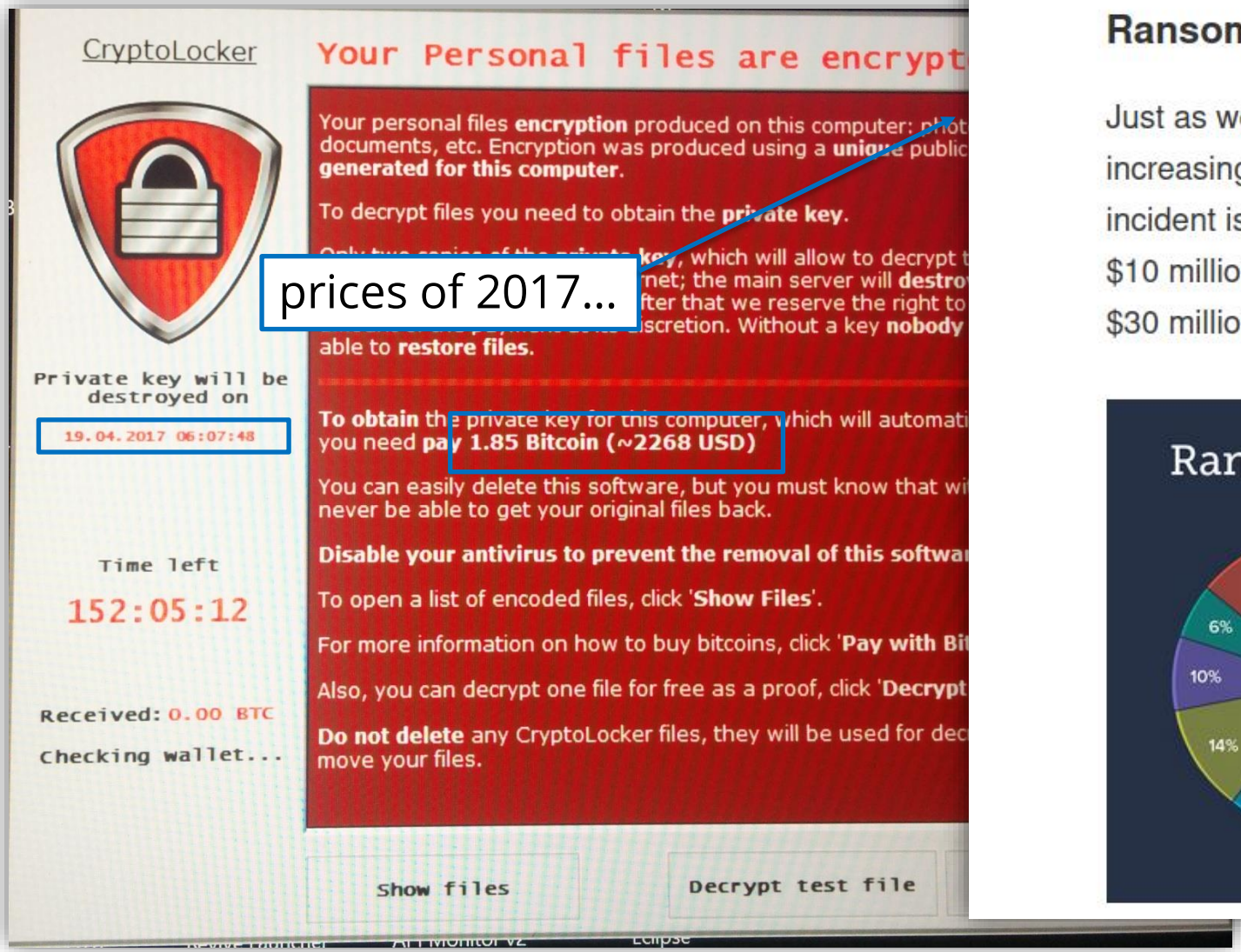



# Ransomware



# Ransomware

2017 → 2021

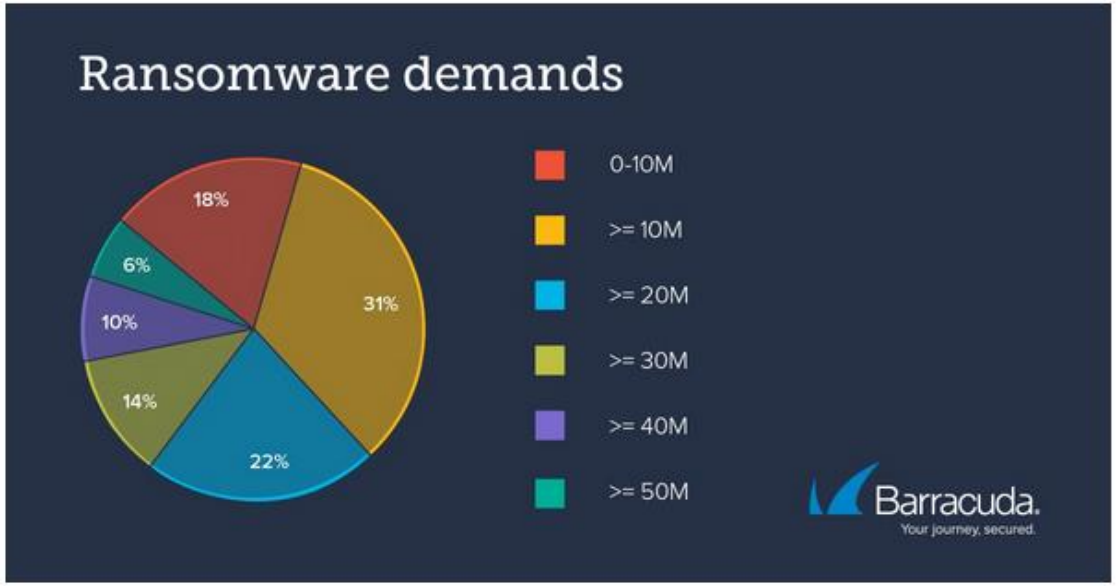



prices of 2017...

https://blog.barracuda.com/2021/08/12/threat-spotlight-ransomware-trends/

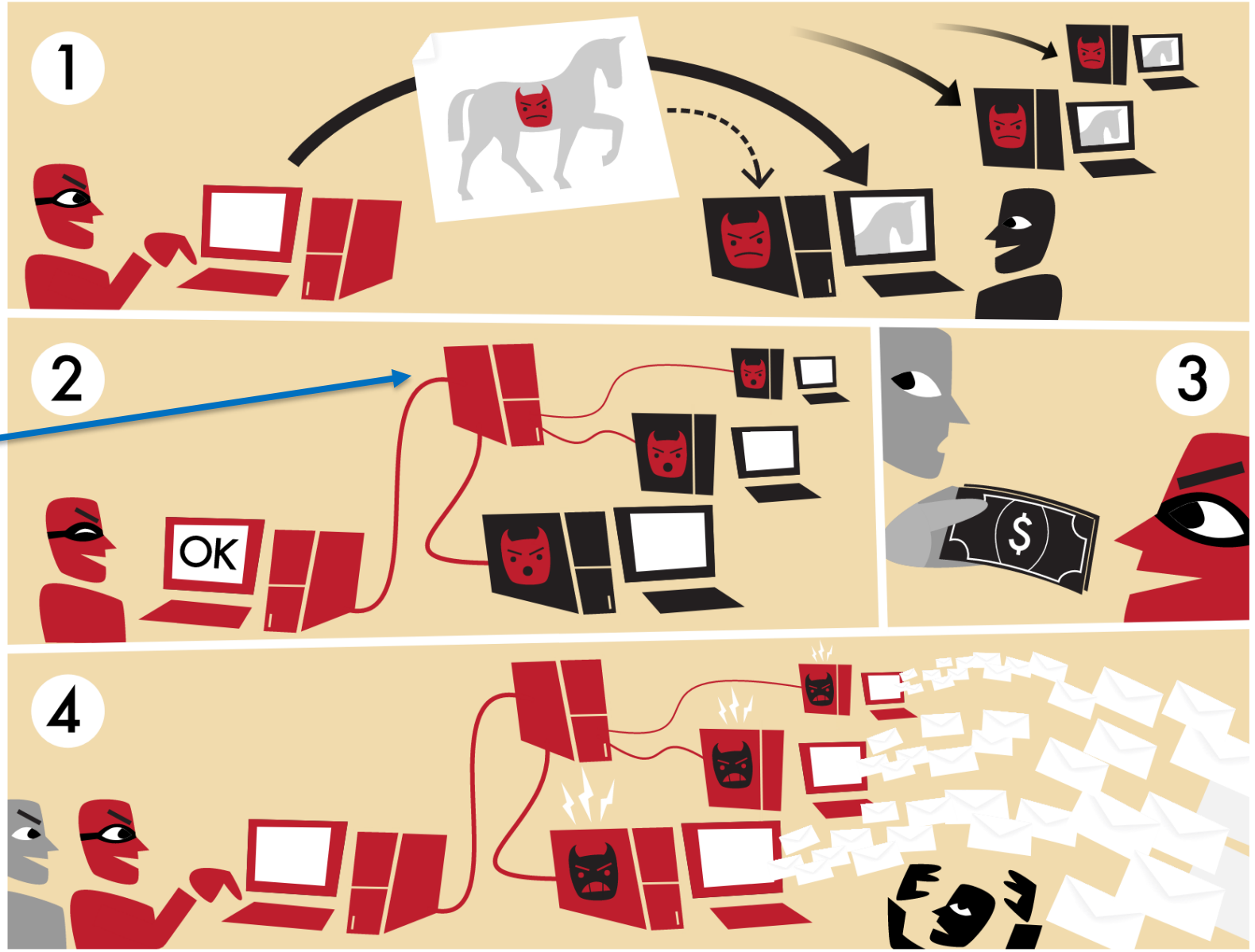
## Ransom payment trends

Just as we have seen in the past years, the ransom amount is increasing dramatically and now the average ransom ask per incident is over $10 million. Only 18% of the incidents had less than $10 million ransom ask, and 30% of the incidents had greater than $30 million ransom asks.



# Botnet

Command and Control Server
(aka C&C Server / C2 Server)




Tom-b, CC BY-SA 3.0, https://commons.wikimedia.org/w/index.php?curid=9084453

# Data Leakage

- Side channel
  - Attacker places probes → often requires physical proximity
- Covert channel
  - Information leak over channels not intended for communication
- Steganographic channel
  - Communication system to ensure undetectability: “confidentiality of the mere existence of a secret message”


```
bjJNelRkUXYK.ip-over-dns.attacker.org
```

microdot camera

# Attack terminology

(without claim to be complete)

| Term | Description |
|---|---|
| **phishing** | Attempt to take possession of sensitive information;<br>Attacker appears as a trustworthy entity |
| **spear phishing** | Phishing attack directed at specific individuals |
| **malware** | Short for malicious software |
| **Trojan horse** | Malicious software embedded in offensive software |
| **virus** | Malicious code that replicates itself into other files or areas on execution |
| **worm** | Malware exploiting active vulnerabilities in order to infect further software |
| **botnet** | A number of connected programs |
| **C&C server / C2 Server** | Command and control server. Central unit controlling a number of combined bots |

# Further terminology

(without claim to be complete)

| Term | Description |
|---|---|
| **threat** | A possible danger that a security vulnerability exists and could be exploited. |
| **vulnerability** | A weakness that can be exploited |
| **exposure** | Existence of a vulnerability that subject the organization to a threat |
| **exploit** | Specific code that takes advantage of a system vulnerability |
| **0-day (zero-day)** | Vulnerability that is unknown to the vendor yet / Exploit which exploits a yet unknown vulnerability |
| **risk** | Probability that a vulnerability gets exploited and thus causes damage |
| **control** | Protection mechanism that reduces the risk (aka *countermeasure*) |

# Controls

| Control type | Description |
|---|---|
| **Preventive control** | reduce the risk of exploitation (e.g. firewall / seminar) |
| **Detective control** | identify violations and incidents (e.g. monitoring) |
| **Deterrent control** | slow down the attacker (e.g. anti-automation) |
| **Recovery control** | restore system configuration and information assets (e.g. backup) |
| **Compensating control** | alternative way of achieving a task (e.g. master-slave set-up with hot takeover / RAID) |
| **Corrective control** | eliminate a nonconformity (e.g. bugfix / deploy patch) |
| **Corrective action** | eliminate the causes of nonconformities in order to prevent recurrence (e.g. change patch process) |

# Quiz

# FAT vs. Web client

What is the difference between FAT and Web client?

In difference to FAT-clients…

A. … data validation can not be done on client-side on Web-clients
B. … Web-clients communicate using the HTTP-protocol
C. … Web-clients are used for multiple (even attacker-controlled) endpoints with different trust-level
D. … Web-clients need SSL/TLS (https) for confidentiality

# Web application security

Why do we have so many security problems in Web applications?

A. Browsers & Operating systems are not updated regularily
B. Libraries and Standards have so many insecure defaults
C. Web Application Firewalls are to expensive compared to Normal Firewalls
D. Users leave incautious to many data in applications and social networks
E. It is hard to remember complicated passwords and therefore, passwords are generally to simple

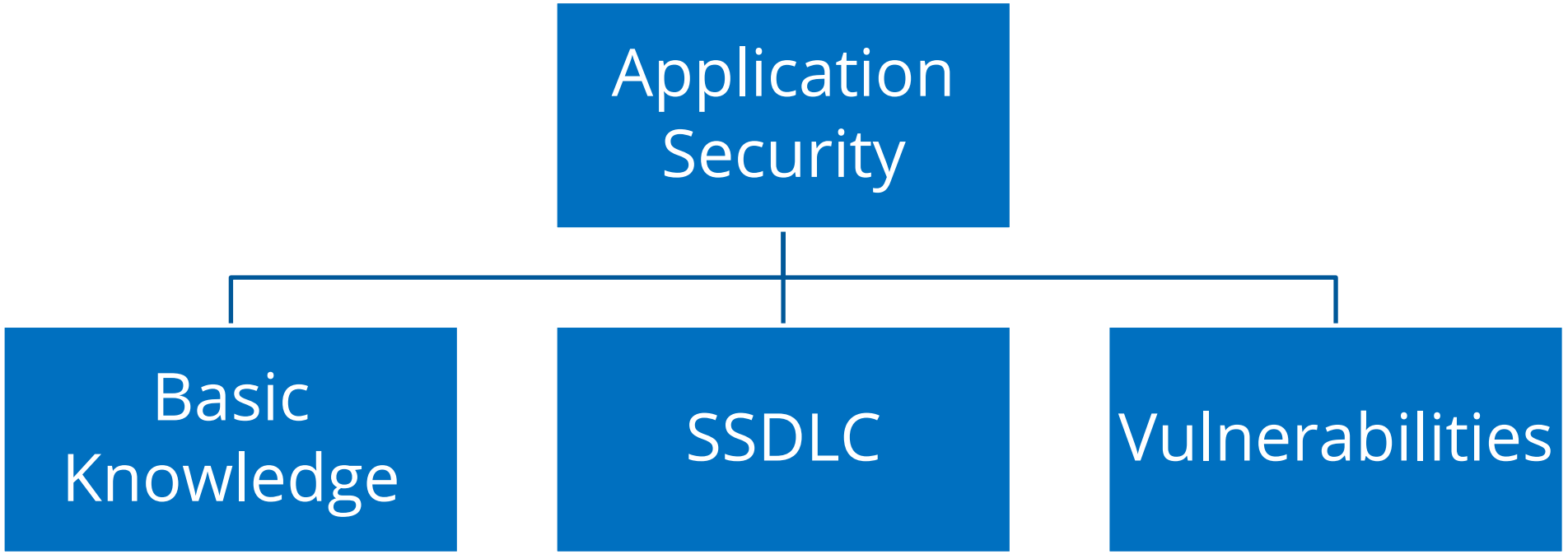
# Terminology

It is important to put a risk on identified weaknesses because…

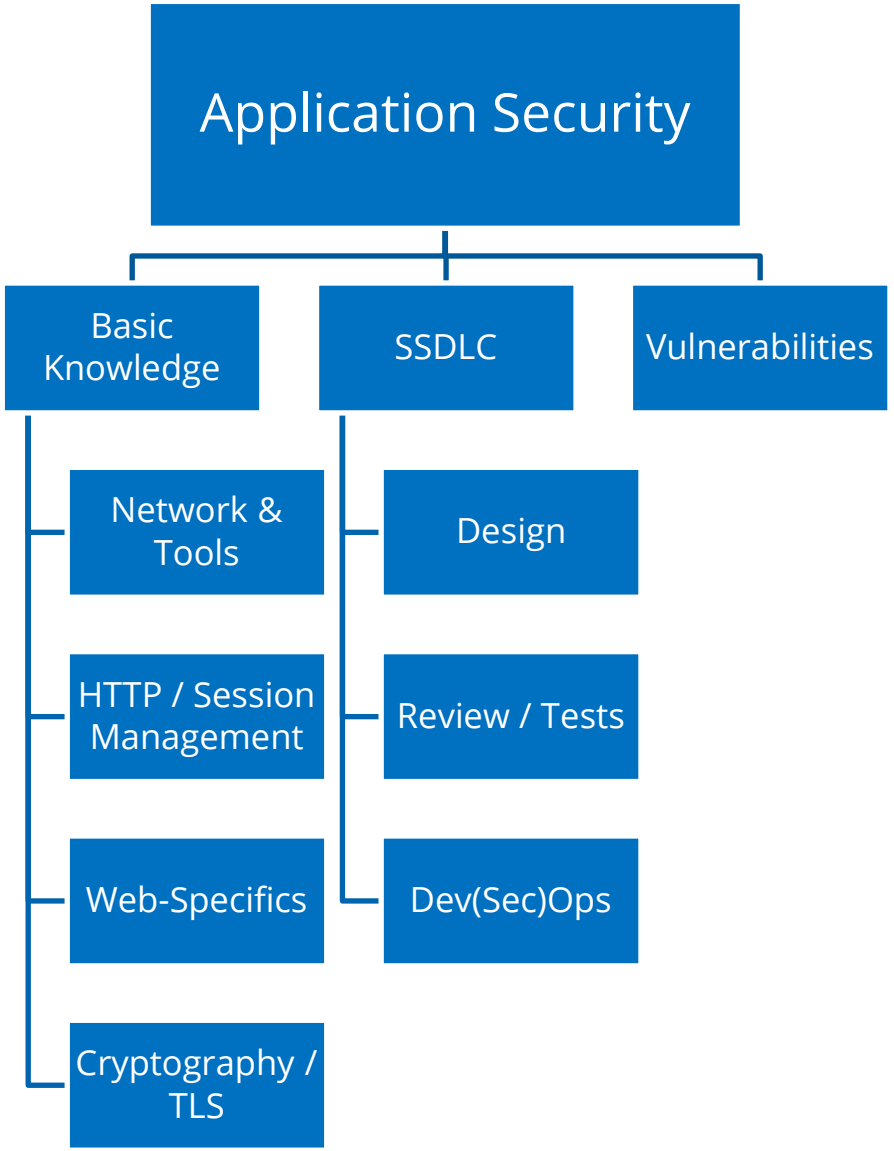
A. It helps to identify which bugs are the important ones and which can be neglected
B. It helps to identify who is responsible for which vulnerability
C. It helps to detect successful exploits
D. It helps to calculate the expected amount of money which will be lost in an attack

# Contents Overview

# Contents



# Contents



# 2021 OWASP Top 10

| | |
|---|---|
| **A1** | Broken Access Control |
| **A2** | Cryptographic Failures |
| **A3** | Injection |
| **A4** | Insecure Design |
| **A5** | Security Misconfiguration |
| **A6** | Vulnerable and Outdated Components |
| **A7** | Identification and Authentication Failures |
| **A8** | Software and Data Integrity Failures |
| **A9** | Security Logging and Monitoring Failures |
| **A10** | Server-Side Request Forgery (SSRF) |

# 5 Layer Model

Layers

| | Level | Content | Examples |
|---|---|---|---|
| 5 | **Semantics** | Preventing Fraud | Phishing Protection Information Disclosure |
| 4 | **Logic** | Securing Workflows and Processes | “Forgot Password” Func.<br>User Lock-out |
| 3 | **Implementation** | Avoiding Implementation Faults leading to Vulnerabilities | Cross-site Scripting<br>SQL Injection |
| 2 | **Technology** | Principles of Secure Coding | Encryption<br>Authentication |
| 1 | **System** | Securing the Software used on the System / Platform | Known Vulnerabilities<br>Configuration Issues |
| 0 | **Network & Host** | Securing the Host and Network | |

# Structuring Vulnerabilities

...by verification step

| OWASP ASVS | |
|---|---|
| V1 | Architecture, Design and Threat Modeling |
| V2 | Authentication |
| V3 | Session Management |
| V4 | Access Control |
| V5 | Validation, Sanitization and Encoding |
| V6 | Stored Cryptography |
| V7 | Error Handling and Logging |
| V8 | Data Protection |
| V9 | Communications |
| V10 | Malicious Code |
| V11 | Business Logic |
| V12 | File and Resources |
| V13 | API and Web Service |
| V14 | Configuration |

...by responsibility

| BSI-Level | |
|---|---|
| 5 | Semantics |
| 4 | Logic |
| 3 | Implementation |
| 2 | Technology |
| 1 | System |
| 0 | Network & Host |

...by control importance

| OWASP Top 10 Proactive Controls | |
|---|---|
| C1 | Define Security Requirements |
| C2 | Leverage Security Frameworks and Libraries |
| C3 | Secure Database Access |
| C4 | Encode and Escape Data |
| C5 | Validate All Inputs |
| C6 | Implement Digital Identity |
| C7 | Enforce Access Controls |
| C8 | Protect Data Everywhere |
| C9 | Implement Security Logging and Monitoring |
| C10 | Handle All Errors and Exceptions |

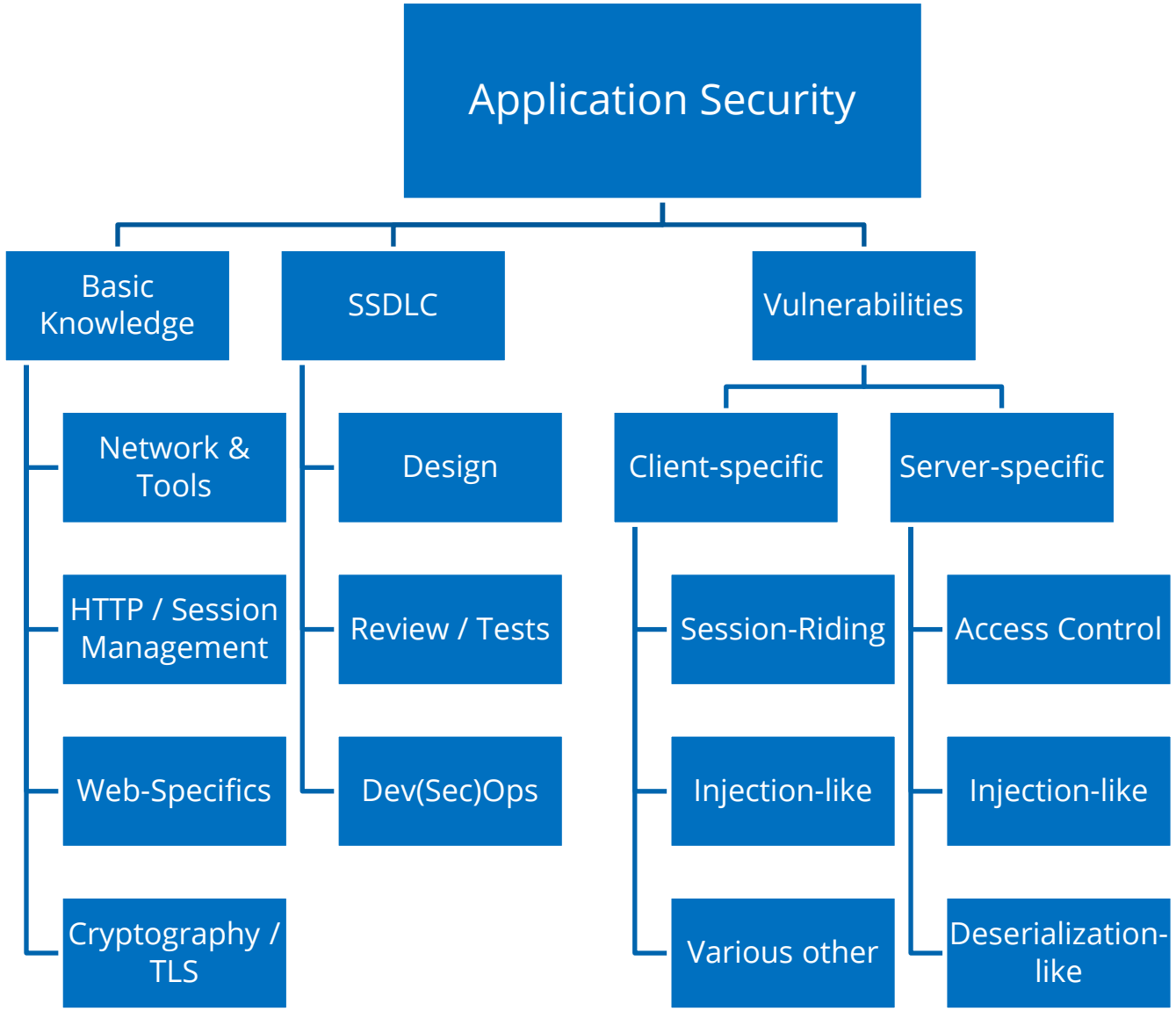
...by occurence

| CWE Top 25 | |
|---|---|
| 1 | Out-of-bounds Write |
| 2 | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') |
| 3 | Out-of-bounds Read |
| 4 | Improper Input Validation |
| 5 | Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') |
| 6 | Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') |
| 7 | Use After Free |
| 8 | Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') |
| 9 | Cross-Site Request Forgery (CSRF) |
| 10 | Unrestricted Upload of File with Dangerous |
| 11 | Missing Authentication for Critical Function |
| 12 | Integer Overflow or Wraparound |
| 13 | Deserialization of Untrusted Data |
| 14 | Improper Authentication |
| 15 | NULL Pointer Dereference |
| 16 | Use of Hard-coded Credentials |
| 17 | Improper Restriction of Operations within th |
| 18 | Missing Authorization |
| 19 | Incorrect Default Permissions |
| 20 | Exposure of Sensitive Information to an Una |
| 21 | Insufficiently Protected Credentials |
| 22 | Incorrect Permission Assignment for Critical |
| 23 | Improper Restriction of XML External Entity |
| 24 | Server-Side Request Forgery (SSRF) |
| 25 | Improper Neutralization of Special Elements used in a Command ('Command Injection') |

| OWASP Top 10 | |
|---|---|
| A1 | Broken Access Control |
| A2 | Cryptographic Failures |
| A3 | Injection |
| A4 | Insecure Design |
| A5 | Security Misconfiguration |
| A6 | Vulnerable and Outdated Components |
| A7 | Identification and Authentication Failures |
| A8 | Software and Data Integrity Failures |
| A9 | Security Logging and Monitoring Failures |
| A10 | Server-Side Request Forgery (SSRF) |

mgm

# Contents

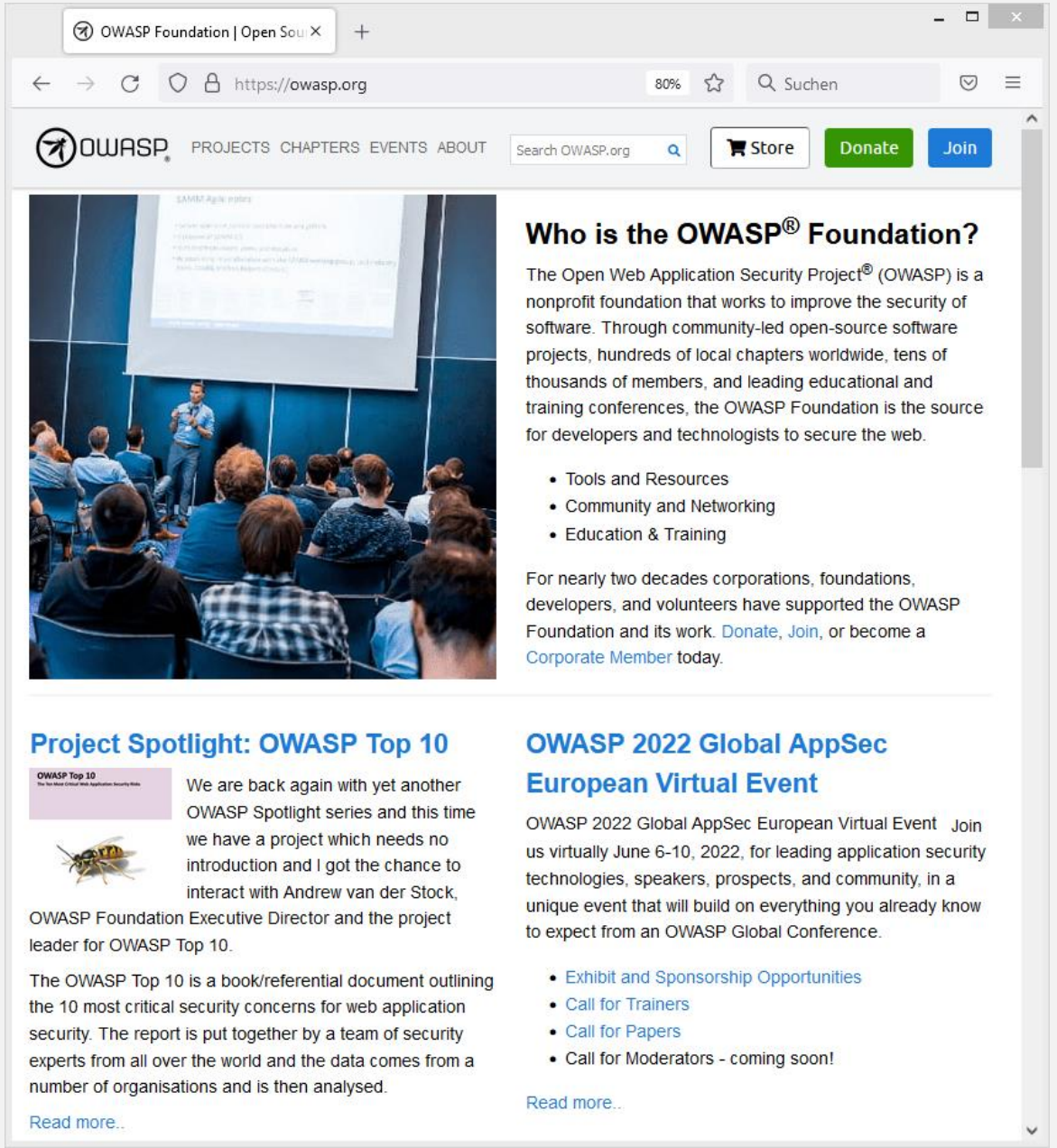


# Resources

# OWASP

**O**pen **W**eb **A**pplication **S**ecurity **P**roject - **www.owasp.org**

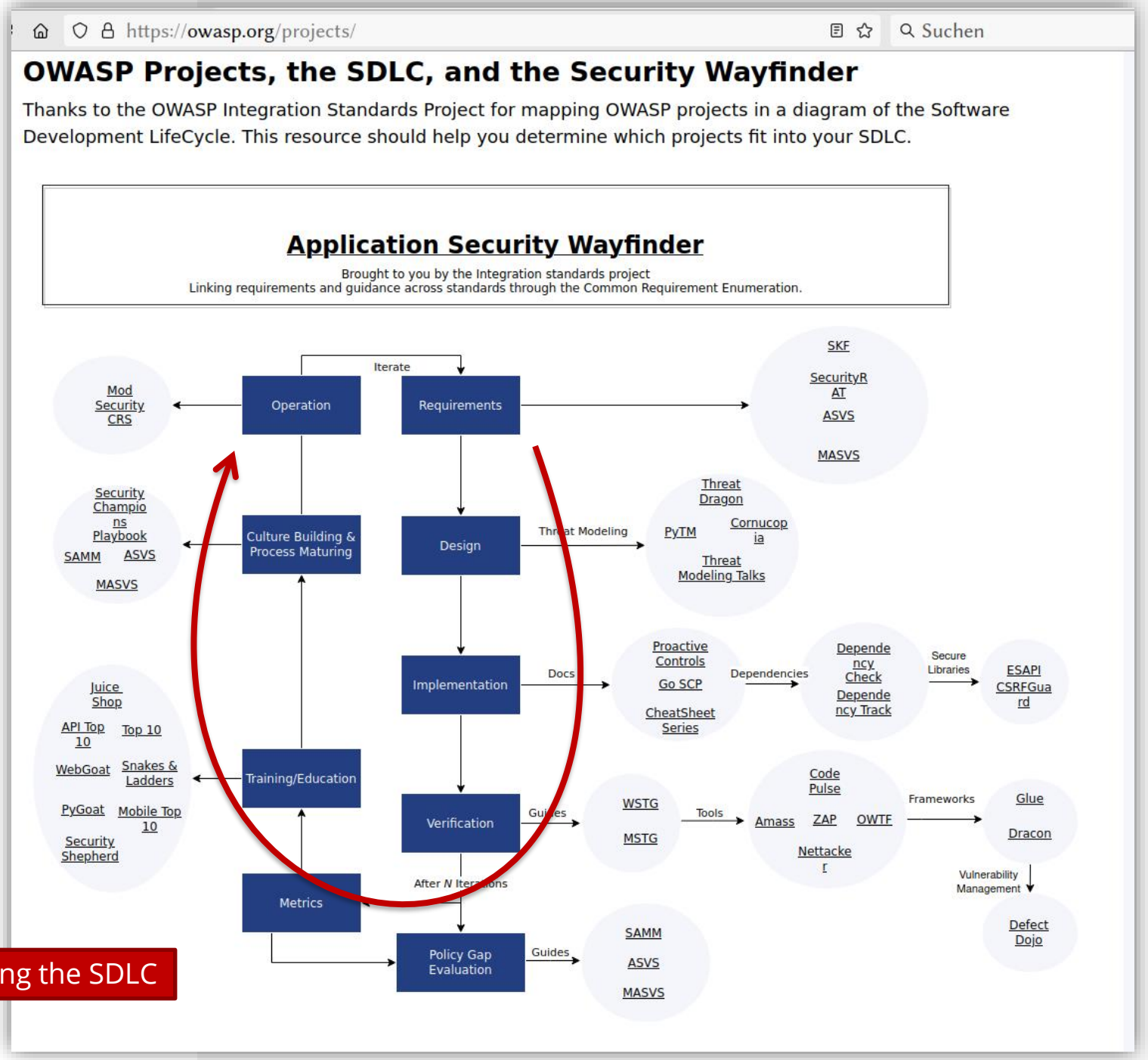
- Chapters
  - Local Discussions (aka Stammtisch)
  - Mailinglists
- Events
  - Conferences (AppSec EU, Global AppSec)
- Projects
  - Top 10
  - Application Security Verification Standard (ASVS)
  - Cheat Sheet Series
  - Security Testing Guides
  - Software Assurance Maturity Model (SAMM)
  - Zed Attack Proxy (ZAP)
  - Dependency Track
  - Vulnerable Web Applications Directory / Juice Shop
  - ModSecurity Core Rule Set




mgm

# OWASP

Project - Wayfinder




Sorted along the SDLC

mgm

# Summary

- The default-case is often the insecure one

- Security can not be added afterwards
  - It can not be “added” using penetration tests
  - It can not be “added” using source code analysis
  - It can not be filtered on the network

→ It is everyone’s responsibility to build secure applications