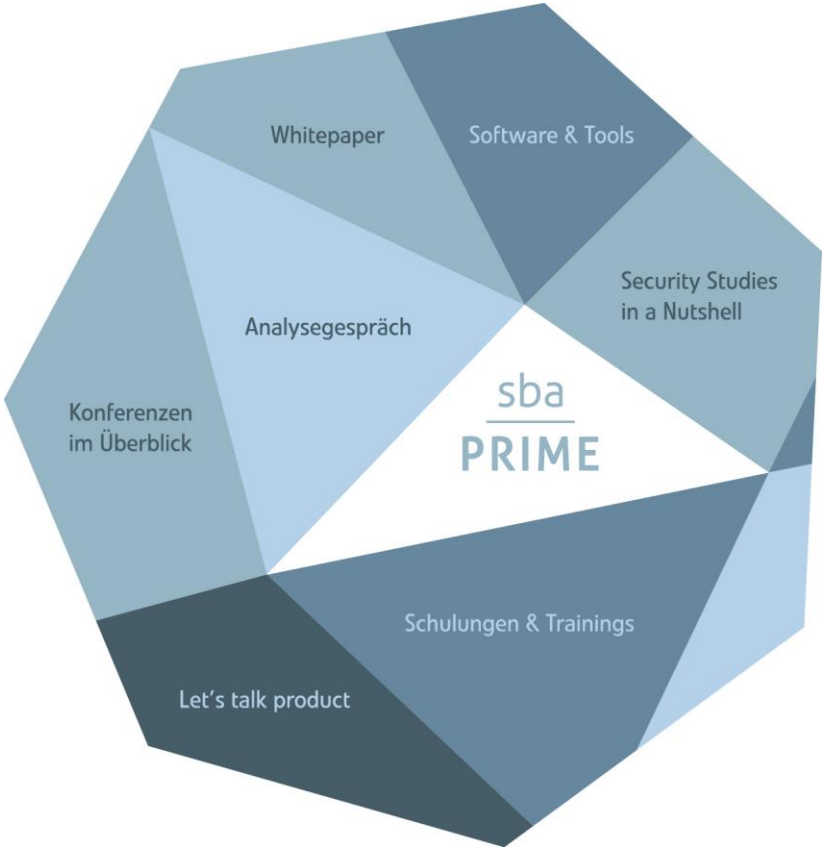
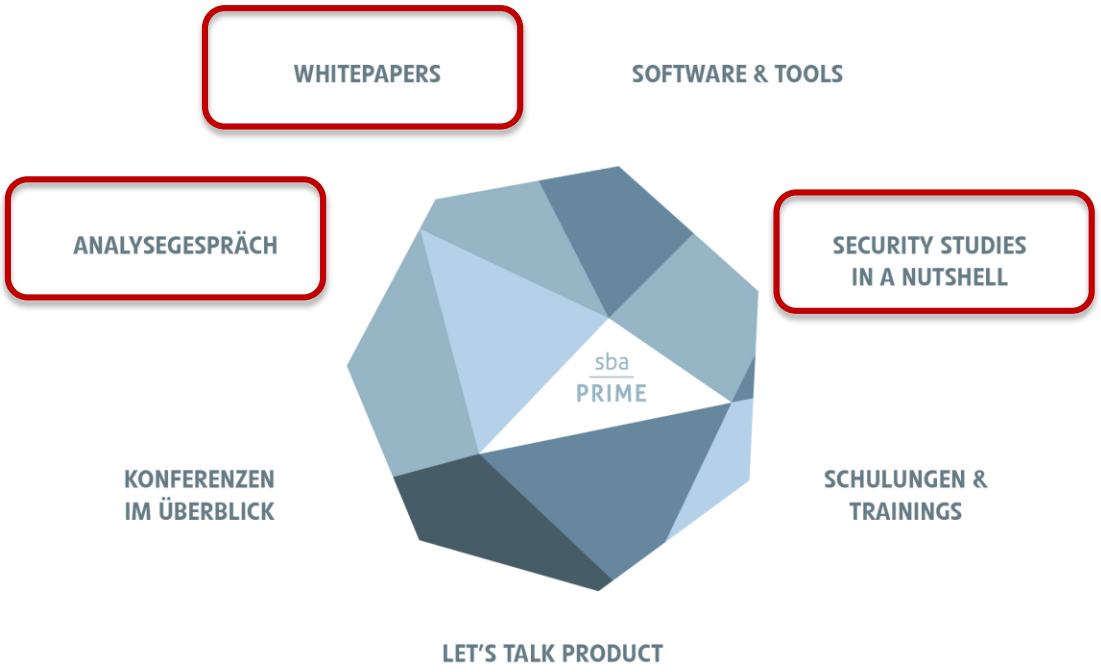

sba
PRIME


Whitepaper
Software & Tools
Security Studies
in a Nutshell
Analysegespräch
sba
PRIME
Konferenzen
im Überblick
Schulungen & Trainings
Let's talk product

INTENTION

VERNETZUNG


WHITEPAPERS
SOFTWARE & TOOLS
ANALYSEGESPRÄCH
SECURITY STUDIES
IN A NUTSHELL
sba
PRIME
KONFERENZEN
IM ÜBERBLICK
SCHULUNGEN &
TRAININGS
LET'S TALK PRODUCT

AKTUALITÄT

Security News 2015-11 | 1

November 3, 2015 · Edit

Hacker extrahiert Merkels Iris Abbild

Dem Hacker „Starbug", der zuvor schon den Fingerabdruck des Deutschen Verteidigungsministers aus einem hochauflösenden Bild nachbilden konnte, ist nun selbiges für die Iris der Deutschen Bundeskanzlerin Angela Merkel gelungen. Die Iris Informationen entnimmt er aus hochauflösenden Bildern wie etwa von Magazinen und druckt diese schließlich mit einem herkömmlichen Laser-Drucker aus.

Details: http://www.planetbiometrics.com/article-details/i/3644/desc/hacker-reveals-how-to-extract-pin-from-any-selfie/

Die größten Cyber-Bedrohungen im Jahr 2015

In Hinblick auf Malware war 2015 wieder ein spannendes Jahr. Im Jänner verbreitete sich ein Trojaner auf Facebook. Zur selben Zeit fanden zielgerichtete Cyber-Angriffe auf syrische Rebellen via Skype statt. Im August präsentierten zwei Sicherheitsforscher den ersten Firmware Wurm für Mac Computer. Auch gehackte Jeep-Autos machten dieses Jahr Schlagzeilen. Rowhammer ist jedoch die bisher gefährlichste Malware dieses Jahres, die eine Schwachstelle in DDR3 RAM-Speicherchips ausnützt. Weitere Informationen unter:

sba PRIME

Isolation of Legacy Systems

A View on Security Concerns for Non-Isolated Legacy Systems

Autors	Christoph Falta and Christoph Mahrl
Version	1.0
Date	05. November 2015

1. Introduction

Legacy systems, a term for out-of-date methods, technologies, computer systems or applications, are considered problematic as continued use of such systems often imply security relevant issues and might therefore impact enterprise operations.

Nevertheless there are possibly compelling reasons for keeping a legacy system that have to be taken into account. These include:

- Costs of migration and redesign of new system
- High availability requirements of legacy systems
- Lack of understanding and documentation of the old system to redesign a new one
- Lack of vendor support to migrate the legacy system to a new platform
- Stability concerns of a new system
- The legacy system already runs satisfactorily

Generally the use of legacy systems is potentially dangerous. Older operating systems or applications may contain vulnerabilities, since the lack of proper security patches being available or applied is putting these systems at risk of being compromised.

Enterprises should always take this riskiness into account as cyber-crime is an increasingly and ongoing topic confirmed by the following surveys and reports:

- In 2014 T-Systems[1] reported that about **92%** of enterprises in Austria expected cyber-crime incidents, **14%** reported about daily attacks.
- According to PWC[2] about **90%** of large organizations had suffered a security breach in 2015, while nearly **three quarters** of small organizations reported a security breach.
- A survey of BITKOM[3] stated, that over **50%** of German companies fell victim to espionage, sabotage or data theft attacks in 2015.
- Kaspersky[4] reported in 2014 that **94%** of companies encountered an external security incident over the last 12 months and **87%** had to deal with an internal security issue.

This whitepaper therefore discusses proactive and reactive security measures that can be implemented in order to mitigate risks exposed by legacy systems. It is intended for organizations where immediate migration is not an option

[1] Cyber-Security Report 2014, T-Systems, 2014

[2] Information Security Breaches Survey, PWC, 2015

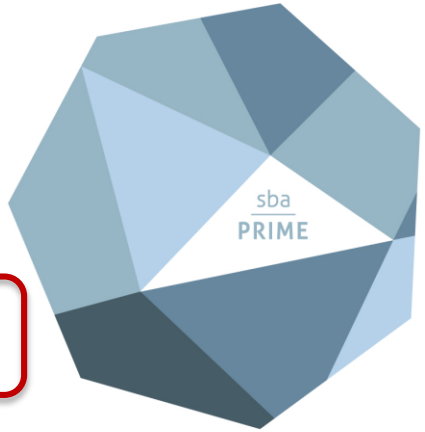
[3] Digitale Wirtschaftsspionage, Sabotage und Datendiebstahl 2015, BITKOM, 2015

[4] IT Security Risks Survey 2014, Kaspersky, 2014

WHITEPAPERS

SOFTWARE & TOOLS

ANALYSEGESPRÄCH



SECURITY STUDIES
IN A NUTSHELL

KONFERENZEN
IM ÜBERBLICK

SCHULUNGEN &
TRAININGS

LET'S TALK PRODUCT

KONFERENZEN

Prime_Best_Of-Usenix_Defcon_2015.pdf - Foxit Reader

FILE HOME COMMENT VIEW FORM PROTECT SHARE FOXIT CLOUD HELP

Prime_Best_Of-Usenix... | Prime_Android_Secu...

Stop ID Theft Secure Attachments

sba PRIME

PRÄSENTATION

Best of BlackHat USA, DEFCON, Usenix Security 2015

sbaPRIME

BlackHat Briefings 5-6.Aug, DEFCON 6-9.Aug, Usenix Security

sbaPRIME

BlackHat USA

- Trainings (4 Tage)
- Briefings (2 Tage)
  - US$ 1800-2600
  - 8 parallel Tracks + 10 Tool Tracks
  - Business Hall
- Keynote (Jennifer Granick)
  - We currently accept censorship, because it only affects marginal groups

sbaPRIME

BlackHat USA

- Vorwort: LibStagefreight
- Android state of the Union (Adrian Ludwig)
- Neues Update Programm: Security Updates für Nexus jedes Monat für 3 Jahre; LG & Samsung folgen
  - PHA – Potential Harmful Application
  - Extensive data collection
    - Looking for high risk devices
    - Rare App collection
      - Targeted Attacks
    - Huge geographical differences (e.g. China, Russia)

sbaPRIME

sbaPRIME

sbaPRIME

1 / 19 45.21%

Prime_Android_Security_Symposium.pdf - Foxit Reader

FILE HOME COMMENT VIEW FORM PROTECT SHARE FOXIT CLOUD HELP

Prime_Best_Of-Useni... | Prime_Android_Securi...

Create PDF from Office Convert PDF to Office

sba PRIME

PRÄSENTATION

Android Security Symposium Recap

sbaPRIME

General Android Security

- No more all powerful root user > 5.0
  - SELinux Policies
  - Makes rooting harder...
- In newer versions Non-PIE binaries are banned
  - Makes ASLR more efficient
- ... A lot more stuff (ASLR, NX, RELRO, StackCanaries, FORTIFY_SOURCE, ...)
- Two interesting talks:
  - Lessons from the trenches: An inside look at Android security, Nick Kralevich, Android Security, Google
  - Android security architecture, Nikolay Elenkov, Sarion Systems Research, Tokyo, Japan)
    - Also has a nice blog on Android Security at http://nelenkov.blogspot.co.at/

sbaPRIME

Android Sandboxes – Of Course ...

- Improving mobile security with forensics, app analysis and big data Andrew Hoog, NowSecure, Oak Park, IL, USA
  - App Analysis Sandbox
  - Analysed about 600.000 apps
  - Plan to make their data open to the public!
- ANANAS - ANalyzing ANdroid ApplicationS, Dieter Vymazal, University of Applied Sciences Upper Austria, Hagenberg, Austria
  - Modular Sandbox

sbaPRIME

Mobile Malware Tracker

- Focused on communication channels and C&C Servers
  - Web and SMS based
- Nice overviews and statistics on what is hosted where
- If you want to know more about Malware distribution:
  - A walk through the construction of the first mobile malware tracker, Federico Maggi, Politecnico di Milano, Italy
  - DroydSeuss[1]

[1] http://ds.andrototal.org/

sbaPRIME

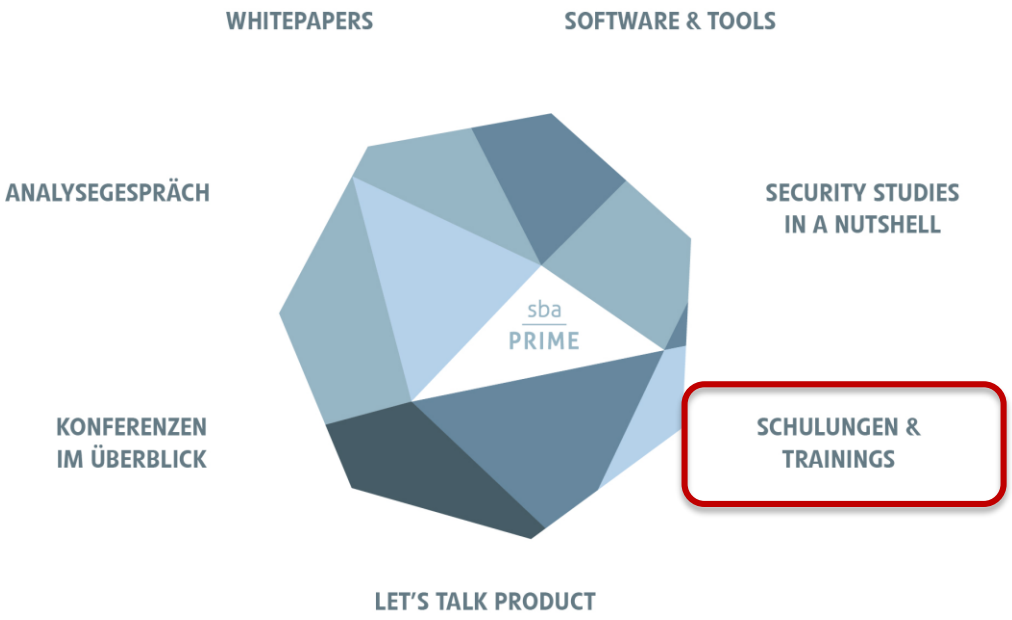
Usable Security is an Issue

- Problem with input on mobile devices
  - 15% of users drop out, when they have to enter a Captcha
  - This is bad if your income depends on amount of users
- Phone Lock/Unlock
  - Again Usability vs. Security
  - Lock Timeout/Unlock Method could be changed based on environment
- Still an unsolved Problem/Work in Progress...
- If your are interested in Usable Security, this might be for you:
  - The quest for usable security, N. Asokan, Aalto University and University of Helsinki, Finland

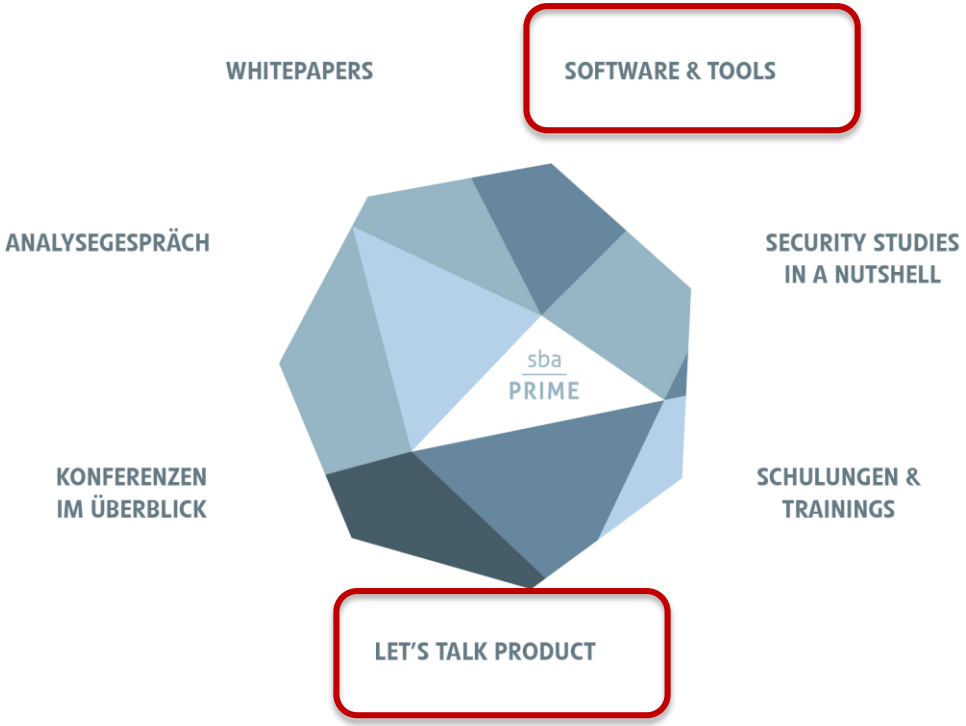
sbaPRIME

sbaPRIME

1 / 12 45.21%



SCHULUNGEN & TRAININGS



SOFTWARE & TOOLS

sbaPRIME

prime.sba-research.org

sba PRIME

News

Neue Whitepapers und Konferenzinhalte online!

November 5, 2015 · Edit

Whitepapers:

- Sicherheitsstrategien für Legacy Systeme
- SharePoint Security in a Nutshell

Konferenzzusammenfassungen:

- Android Security Symposium 2015: Prime_Android_Security_Symposium.pdf
- Black Hat / USENIX / DEFCON 2015: Prime_Best_Of-Usenix_Defcon_2015.pdf

Gerne werden Ihnen diese Whitepapers und/oder Konferenzzusammenfassungen sowie weiterführende Informationen im Rahmen der Analysegespräche persönlich vorgestellt und präsentiert.

Security News 2015-11 | 1

November 3, 2015 · Edit

Hacker extrahiert Merkels Iris Abbild

Überblick Leistungsumfang pro Jahr

WHITEPAPERS

Detaillierte Aufbereitung aktueller IT-Security-Themen als Whitepapers z.B. Sicherheitsstrategien für Legacy Systeme

SOFTWARE & TOOLS

Softwareprodukte aus dem Forschungsumfeld ohne zusätzliche Lizenzkosten z.B. sbox, Nessus-Data-Cube

ANALYSEGESPRÄCH

Analysegespräch mit unseren Expert/innen im Ausmaß von 1,5 Personentagen zu einem Security Thema Ihrer Wahl

SECURITY STUDIES IN A NUTSHELL

Nationale und internationale Studien zum Thema Informationssicherheit kompakt und aussagekräftig

KONFERENZEN IM ÜBERBLICK

Zusammenfassung der wichtigsten IT-Security-Konferenzen weltweit

SCHULUNGEN & TRAININGS

Zwei Kursteilnahmen (z.B. Secure Coding, CISSP, Windows Hacking)

LET'S TALK PRODUCT

Präsentation und technische Evaluierung von innovativen Softwarelösungen im IT-Sicherheitsbereich

PRIME@SBA-RESEARCH.ORG
PRIME.SBA-RESEARCH.ORG

Gernot Goluch

SBA Research gGmbH
Favoritenstraße 16, 1040 Vienna, Austria
GGoluch@sba-research.org


sba
PRIME

Security Studies in a Nutshell

Challenge: Being Up To Date

Ich habe keine Zeit mich zu beeilen.

Igor Strawinsky

Why Security Surveys in a Nutshell?

- I want to be **informed & prepared**
  - I want to **"benchmark"** against others
  - I need statistics and figures to **substantiate** my intentions & plans
  - I want to see **trends**
  - I want to review or align my **strategy**

- The challenge: there are **heaps of surveys** (and reports) with different content, focus and quality = no time

What Can You Expect?

- Valuable **preselected and preprocessed** information that **saves your time**
  - Overview of existing surveys
  - Overview which topics are discussed where
  - Comparison of specific topics across surveys
  - Focus on hot topics
  - Indication of surveys' quality

The Menu

1) Included surveys & topics covered
2) Selected hot topics
   - Which security measures are implemented?
   - The current status regarding mobile security?
   - What about cyber risk insurances?
3) Special excursion: “Bias in (Security) Surveys”
   - What to consider when reading a survey?

Security Studies in a Nutshell

Survey Overview

Included surveys & topics covered

Processed Surveys

- Currently, 32 surveys (and reports) within scope
  - Approx. 2.000 pages

- At the moment **17 in detailed elaboration**

10

6

2

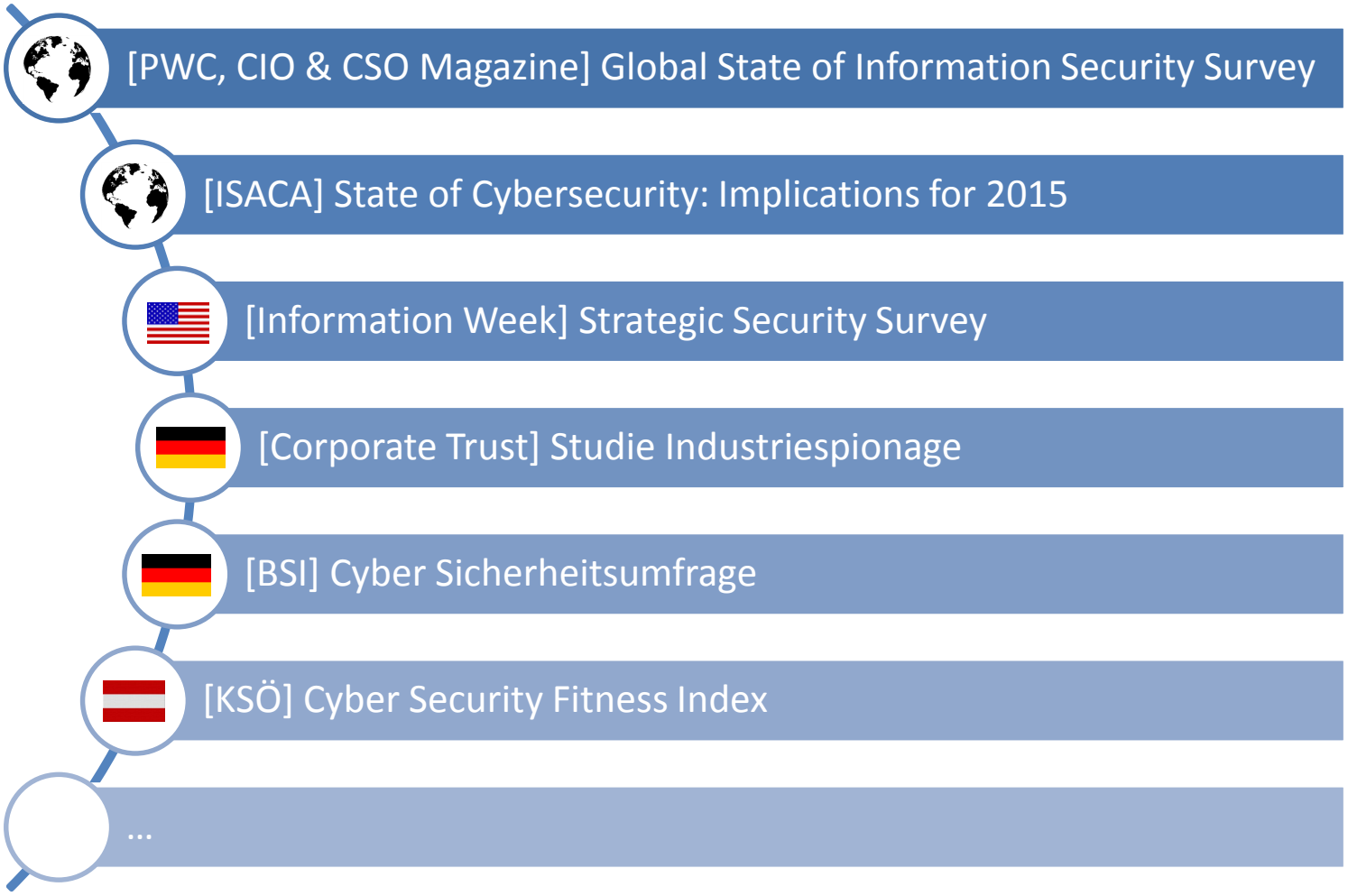
Topics Covered - Excerpt

- Security **Spending**
- Perceived **Threats**
- **Incidents** & Breaches
- **Costs** of Security Breaches
- Implemented **Security Measures**
- **Importance** of IT Security
- Threat **Agents**
- **Insider** Threat
- **Mobile Devices** Threat & Security Measures
- Incident/Breach **detection & time to discovery**
- Biggest IT Security **Challenges**
- **Most-Valuable** Security Practices
- **Contingency** Planning
- **Drivers** for Information Security
- **APTs**
- Threat **Intelligence**

Topics Covered - Excerpt

- Security & **External Suppliers/Partners**
- **Vulnerability** Disclosure statistics
- **Spam**
- **Phishing**
- **Malware**
- **DDoS**
- **Exploit Kits**
- Most **Common Attack** Techniques
- Used **Operating Systems**
- **Countries** as source of cyber attacks
- Cyber Attacks **per sector**
- Usage of **Standards**
- Usage of **Cloud and Outsourcing**
- Usage and security verification of **Open Source Software**
- **Heartbleed** and **Shellshock**
- *… and many more …*

Where to find “Implemented Measures”?



Security Studies in a Nutshell

Selected Hot Topics

Security Studies in a Nutshell

Selected Hot Topics

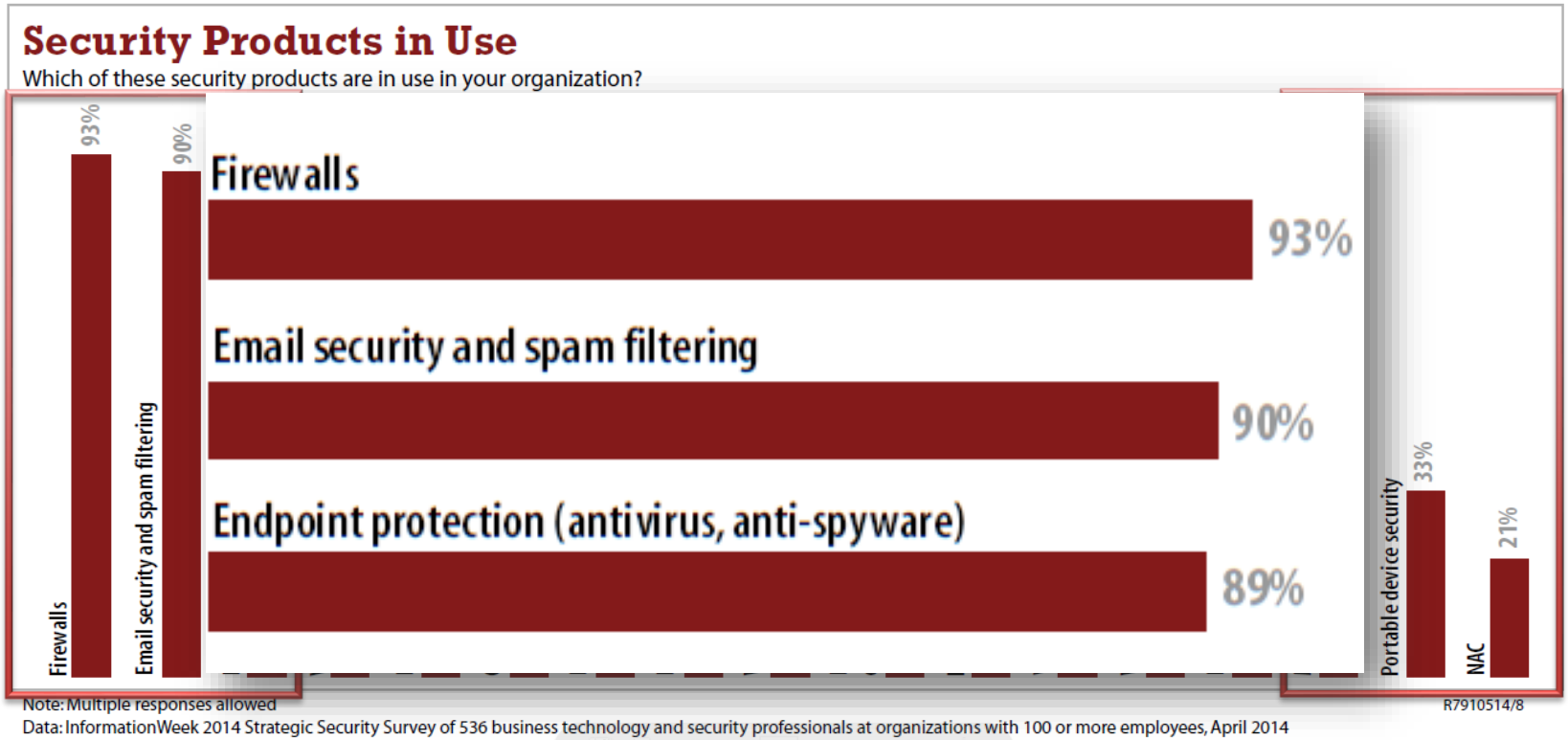
Implemented security measures?

If You are sbaPRIME Member…

- … you will know that the **key security measures** are:
  - Border security
  - Anti malware
  - Passwords
  - Security Awareness

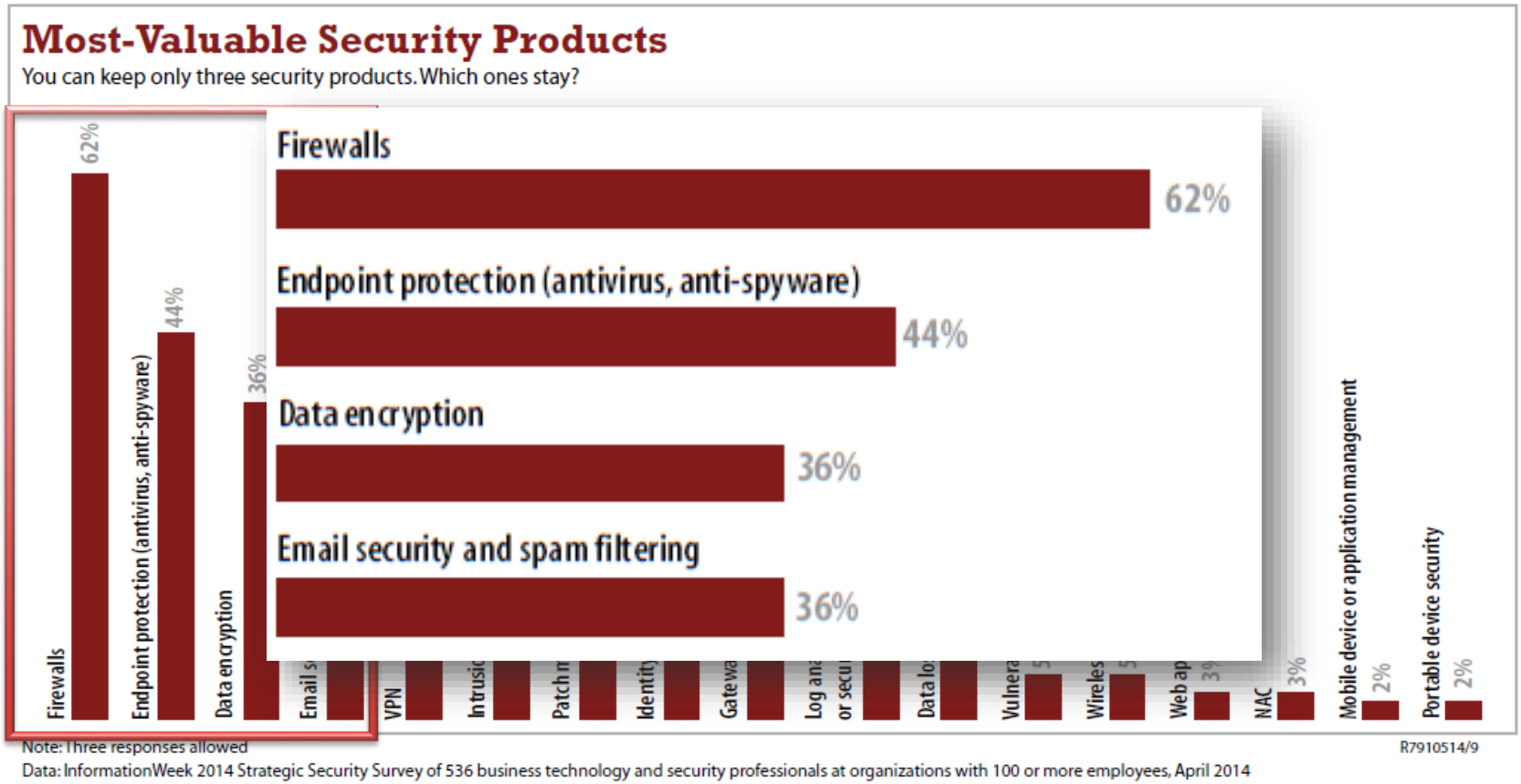
- … you will know that **poorly implemented** measures are:
  - Portable device security
  - Network access control
  - Attacker attribution
  - Monitoring of unapproved cloud services

Usage of Security Products



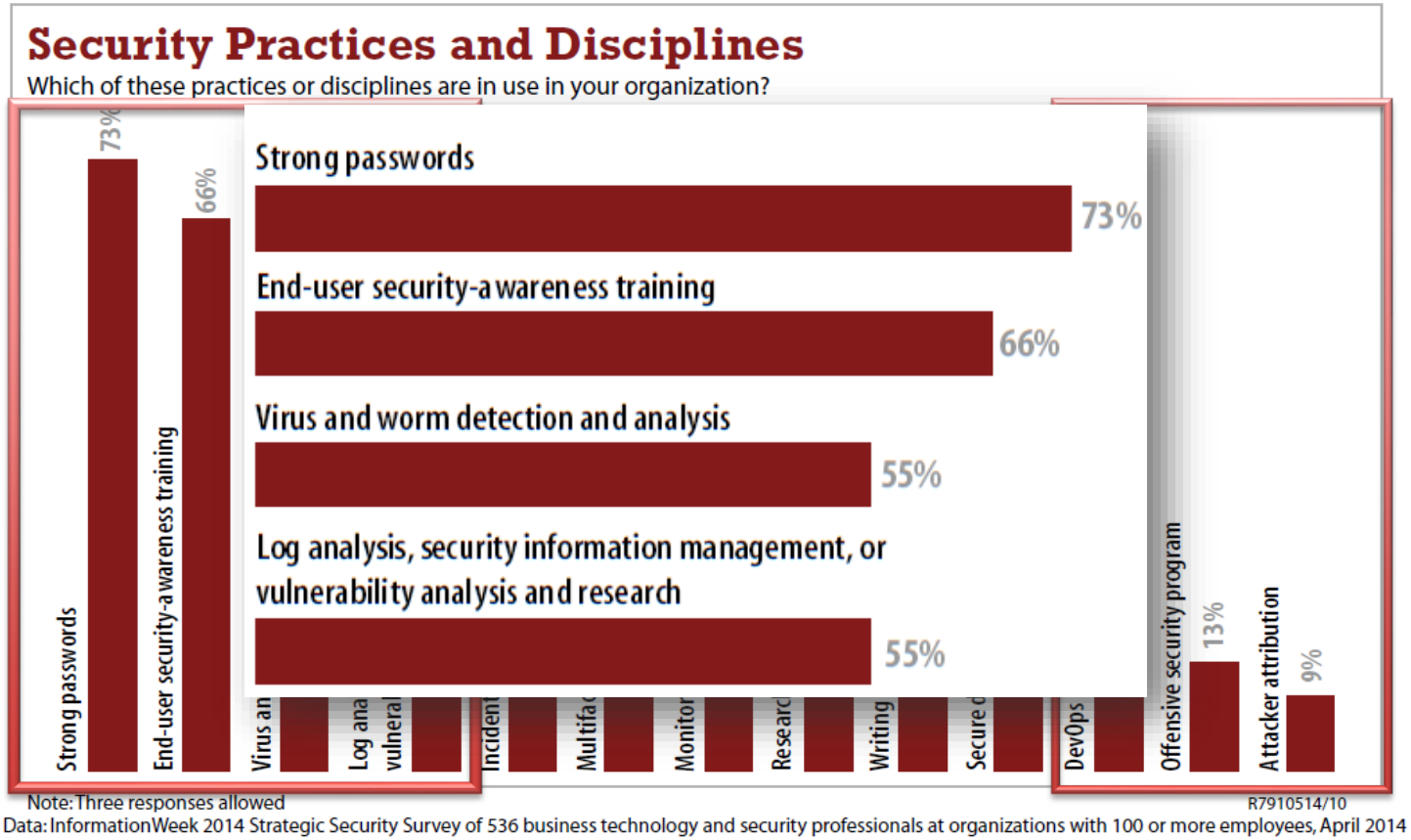
[Information Week Strategic Security Survey, 2014]

If You had to Choose 3



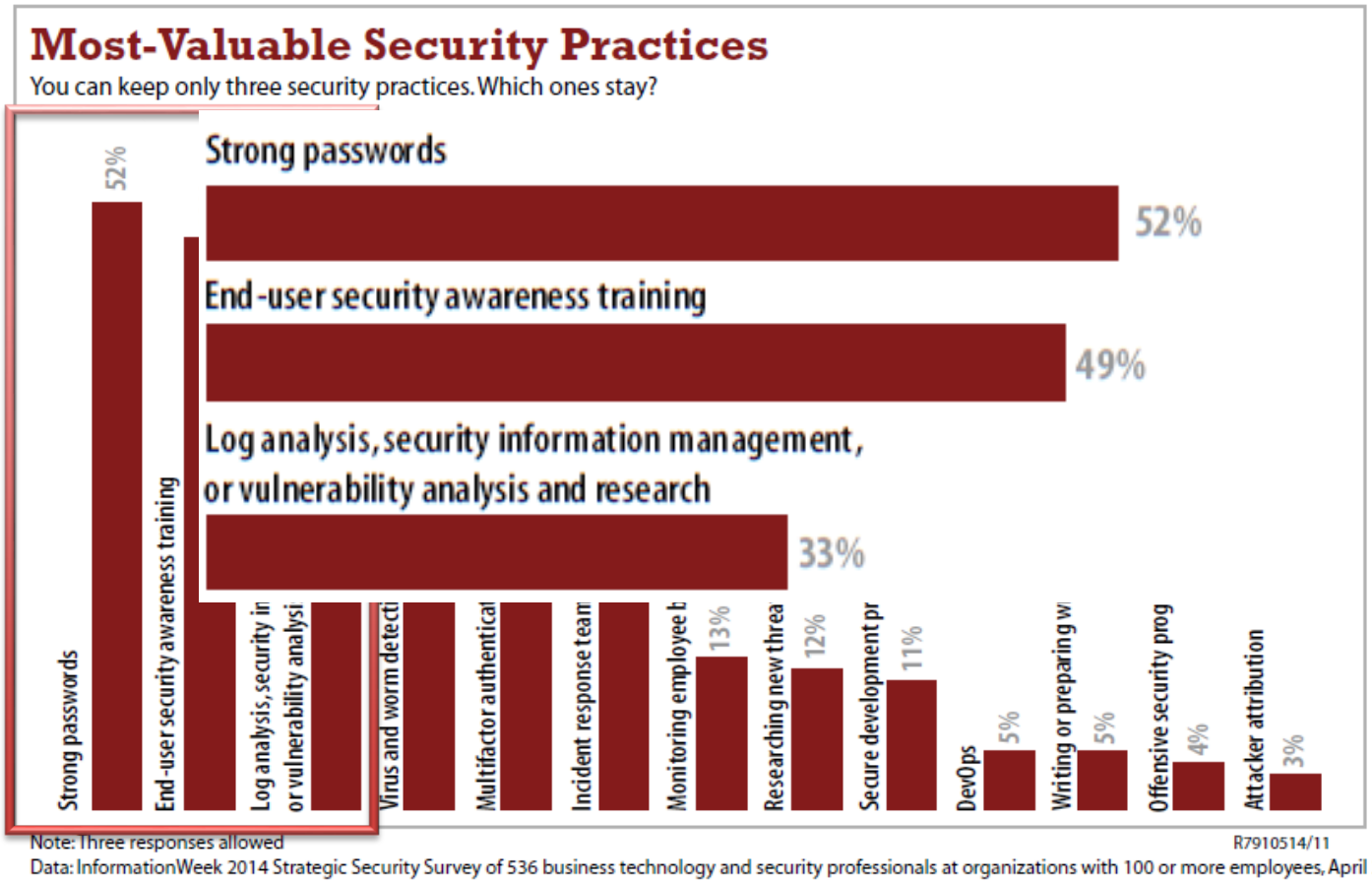
[Information Week Strategic Security Survey, 2014]

Usage of Security Practises



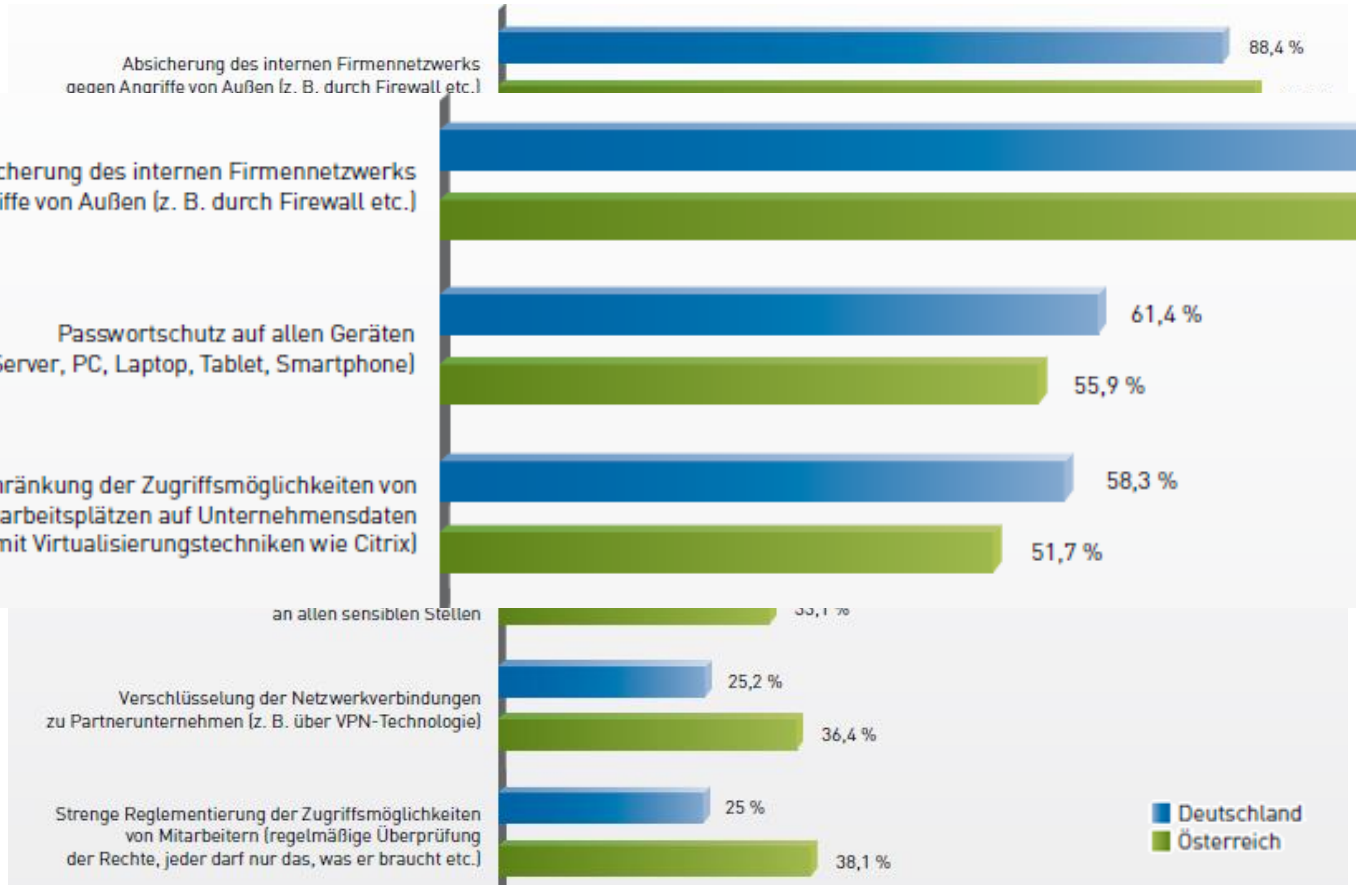
[Information Week Strategic Security Survey, 2014]

If You had to Choose 3



[Information Week Strategic Security Survey, 2014]

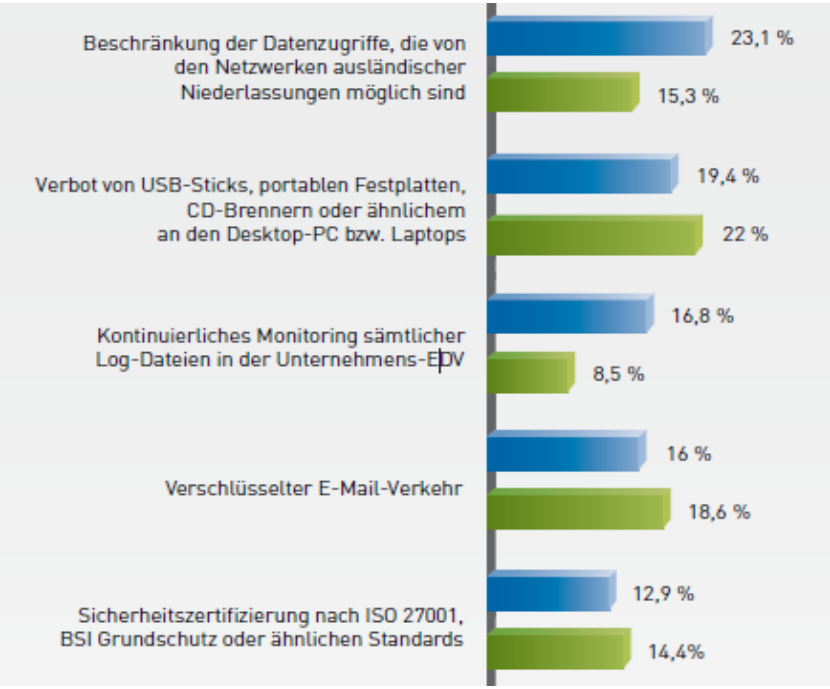
Protection Against Data Leakage

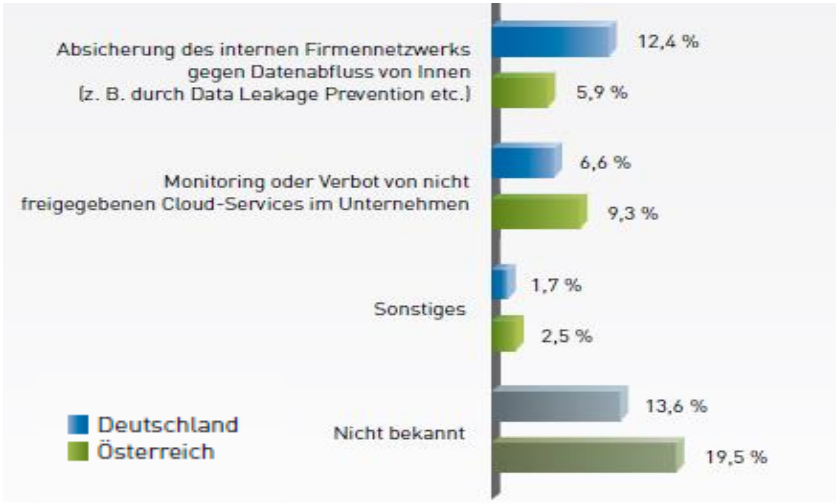


[Corporate Trust: Studie Industriespionage 2014]

Poorly Implemented Security Measures

- **Encryption of e-mail traffic, security certifications, Logging & Monitoring and DLP** only in a **minority** of companies

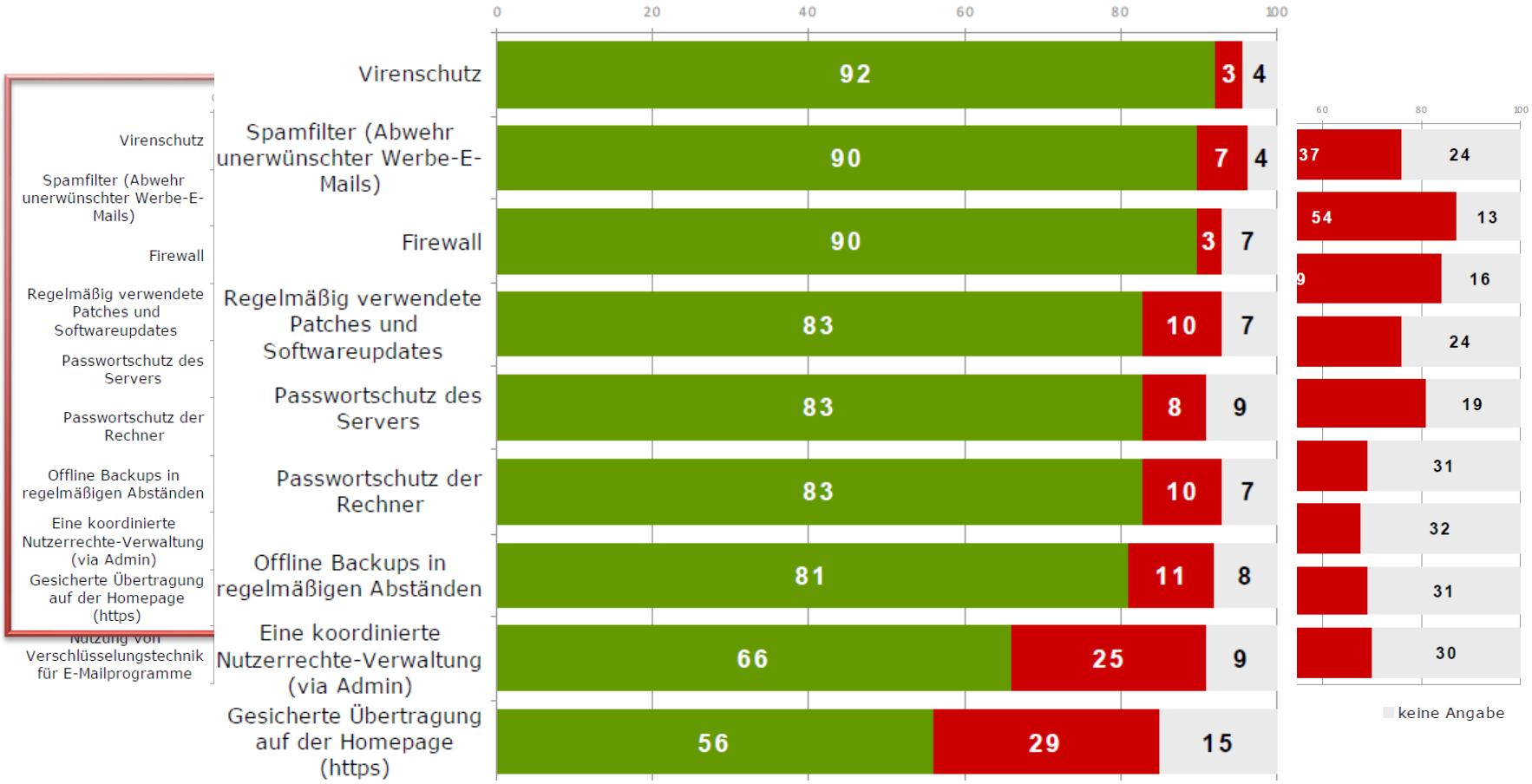




[Corporate Trust: Studie Industriespionage 2014]

sbaPRIME

Implementation >50% in Austrian SME



Security Studies in a Nutshell

Selected Hot Topics

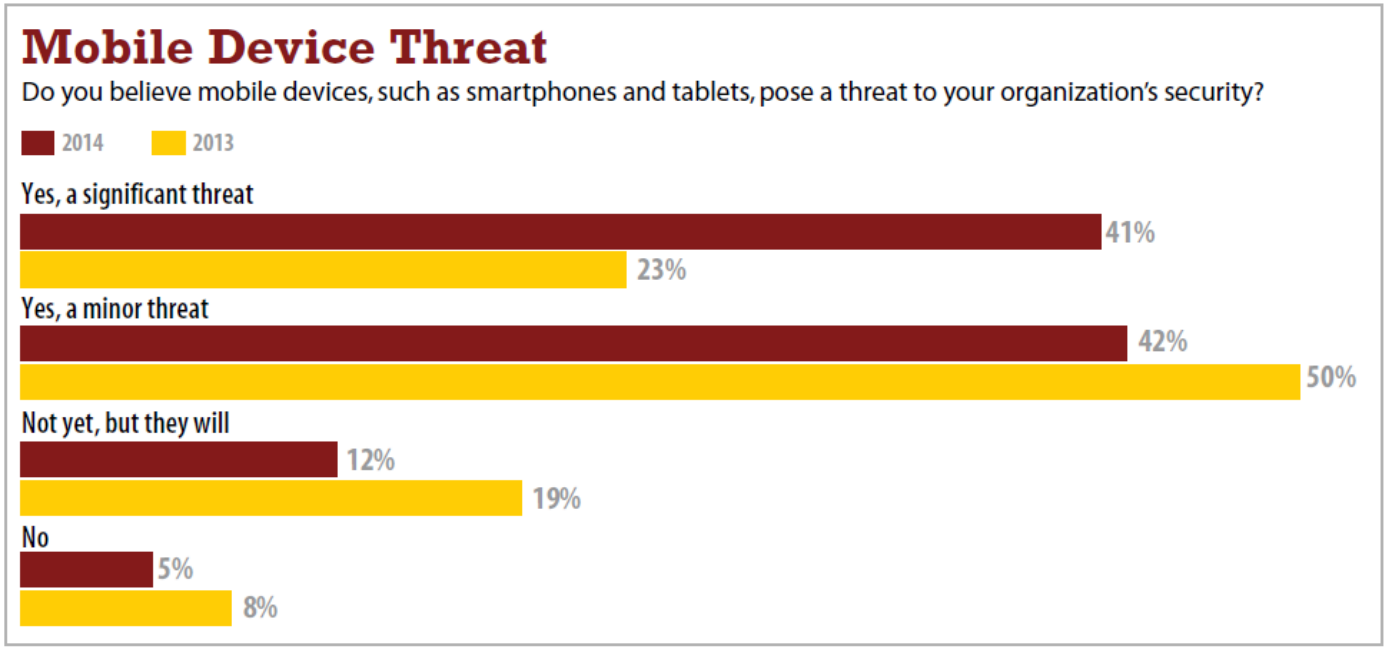
Current mobile security status?

If You are sbaPRIME Member…
… you will know that

- Only **5% think** that mobile devices are **no threat**
- **90% experienced a loss** of mobile devices
- A **mobile security strategy** is the only measure that is implemented by every 2nd organization
- Only a **minority of German and Austrian companies** have a MDM solution or guidelines concerning BYOD
- There is **widespread discontentment** with mobile device security measures

Are Mobile Devices a Threat?

- **40%** of companies believe that mobile devices are a **significant** threat to their organization
- **Only 5%** think that mobile devices are **no threat**



[Information Week Strategic Security Survey, 2014]

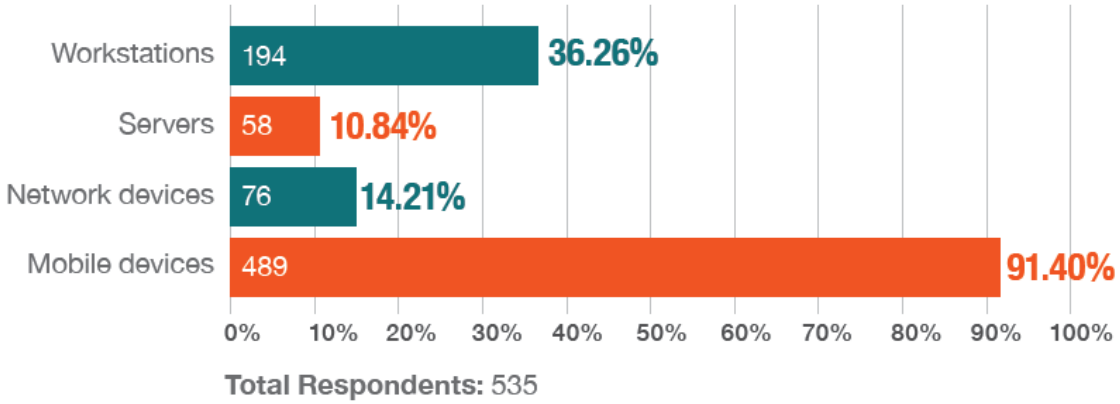
Loss of Physical Assets

- Loss of Mobile Devices **very common**
- Mobile devices **often involved in security breaches**

15% of large organisations had a security or data breach in the last year involving smartphones or tablets.

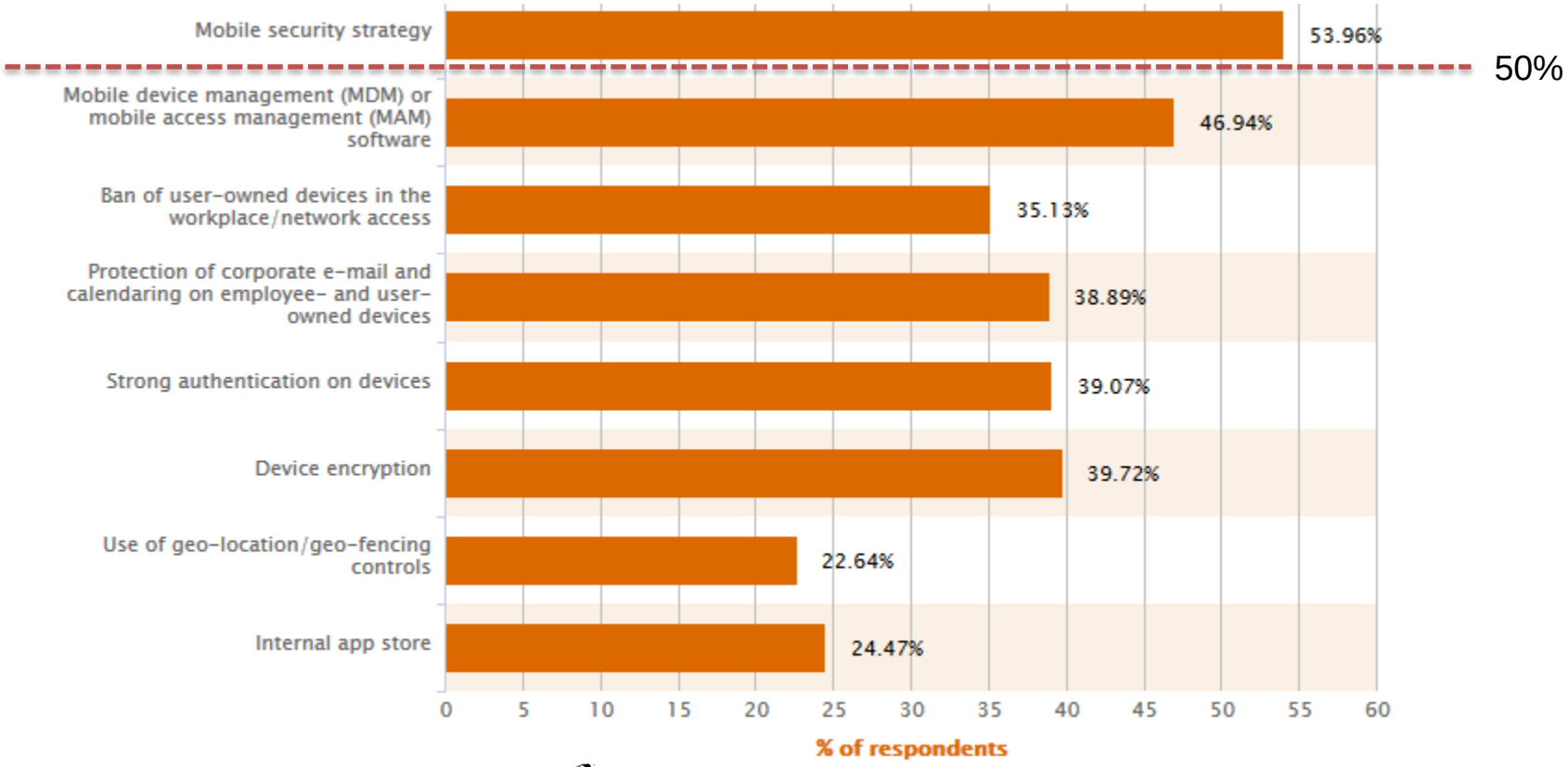
[PWC Information Security Breaches Survey, 2015]

Figure 12—Lost Physical Devices
Has your organization experienced physical loss of assets in 2014?
What type of assets?



[ISACA: State of Cybersecurity: Implications for 2015]

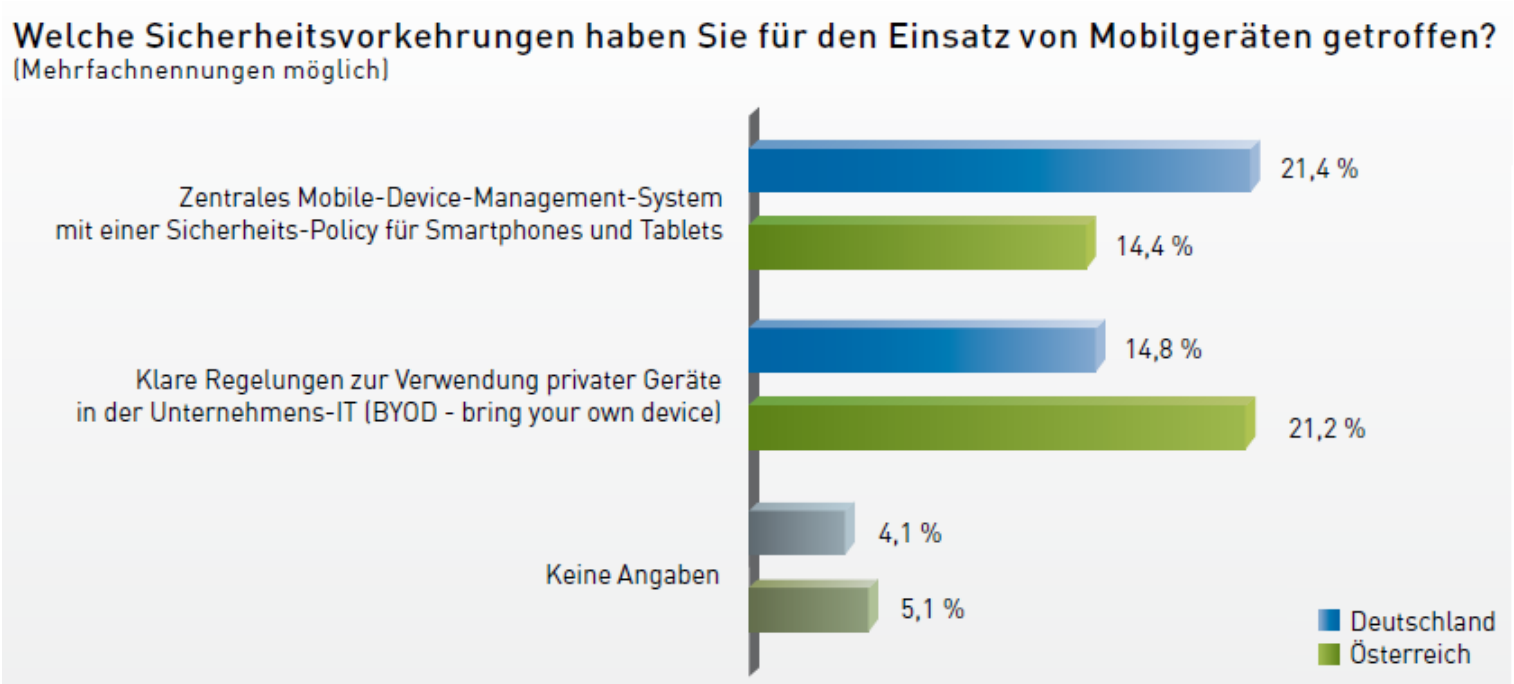
Usage of Mobile Security Measures



[PWC Global State of Information Security, 2015]

MDM in Germany and Austria?

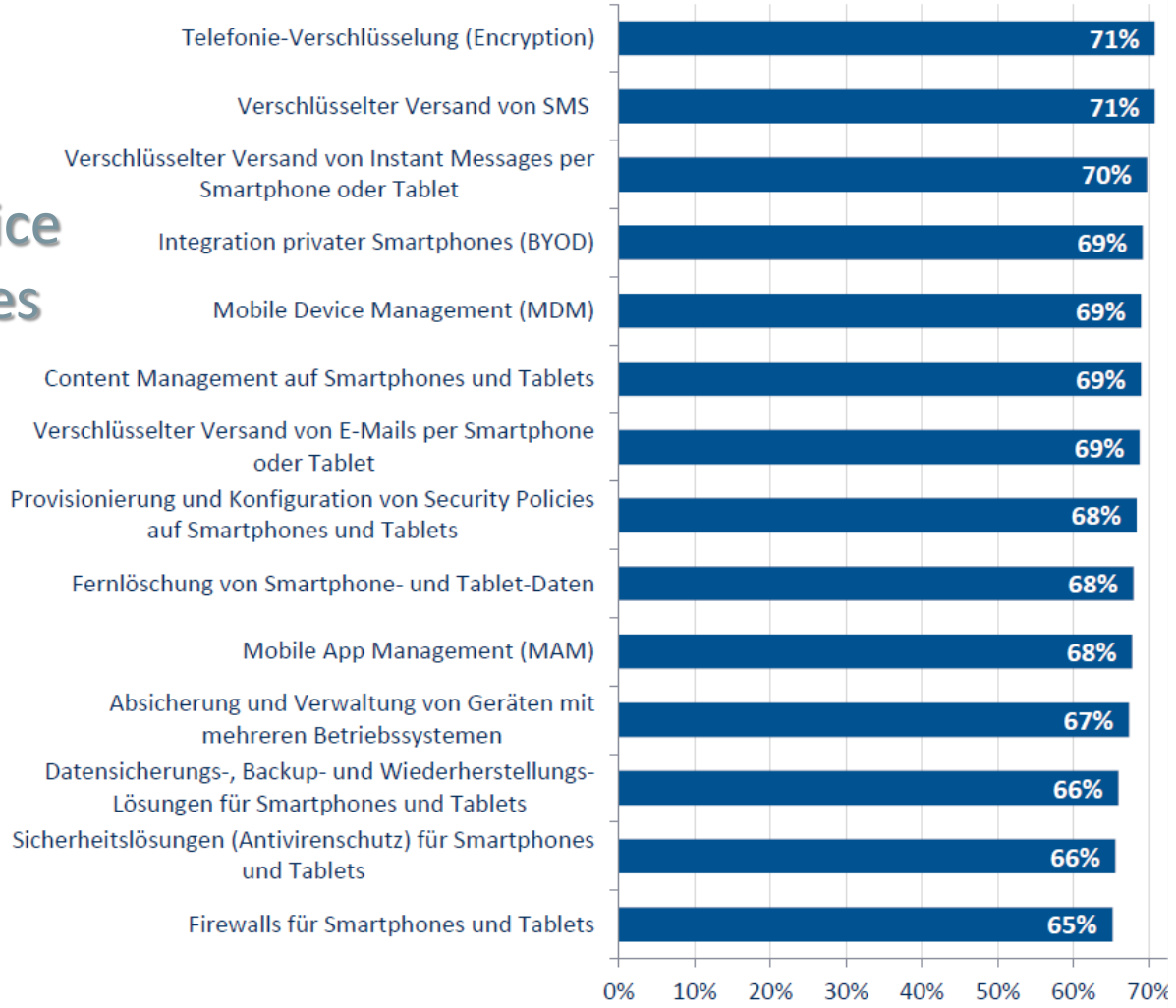
- Only a **minority of German and Austrian** companies have a **MDM solution** or guidelines concerning BYOD



[Corporate Trust: Studie Industriespionage 2014]

Level of Satisfaction?

- Widespread discontentment with mobile device security measures



[Techconsult: Security Bilanz Deutschland, 2015]

Security Studies in a Nutshell

Selected Hot Topics

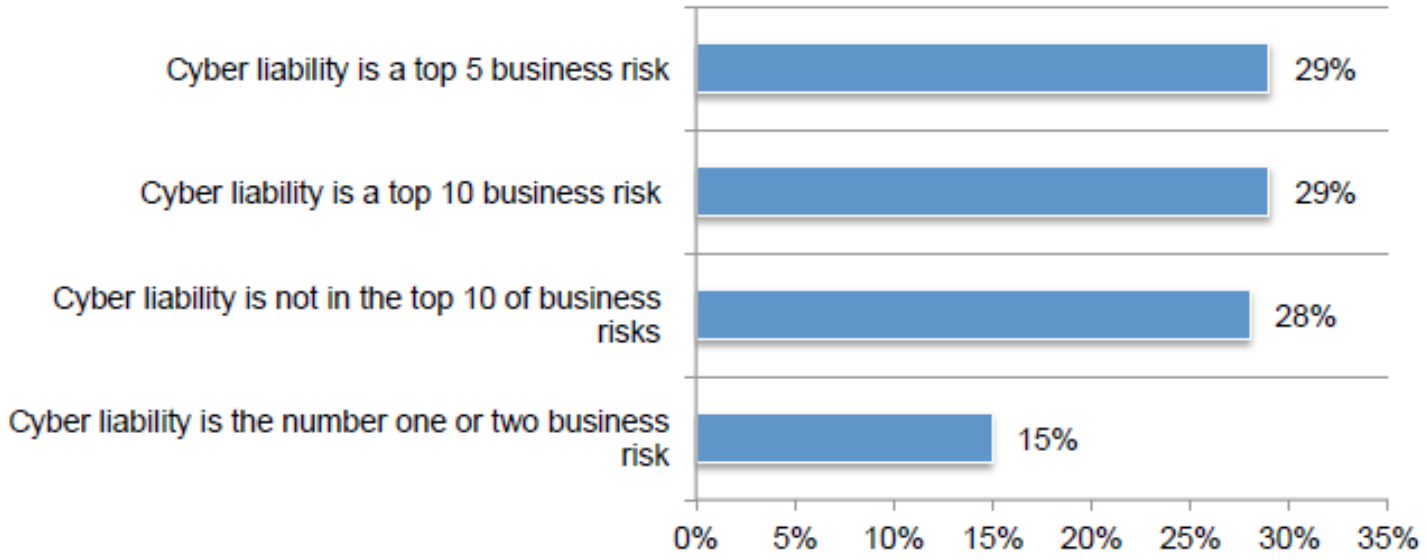
What about cyber security insurances?

If You are sbaPRIME Member…
… you will know that

- Only 1/3 of companies include cyber risks within top 5 business risks
- Cyber security insurances are currently a not widely regarded topic
  - … but they rapidly get more attention
- Currently, nobody “has a clue” how to size the insurance
- In Austria approx. 6% are negotiating an insurance

Cyber Risk Positioning

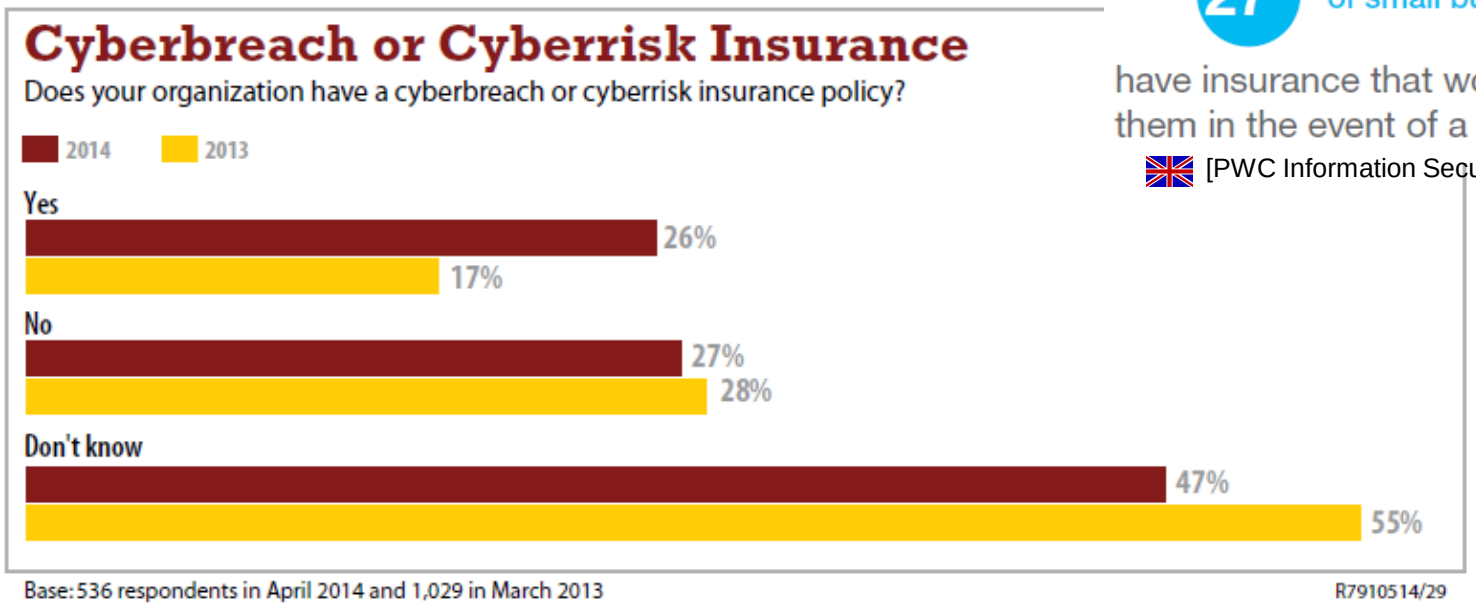
Figure 18. How do cyber risks compare to other business risks?



[Ponemon/Aon Global Cyber Impact Report, 2015]

Usage of Cyber Security Insurances

- Available on the **market for around 10 years**
- **Not yet widely used, but increasing level of attention**
  - Especially in countries with mandatory data breach notification laws



[Information Week Strategic Security Survey, 2014]

39% of large organisations

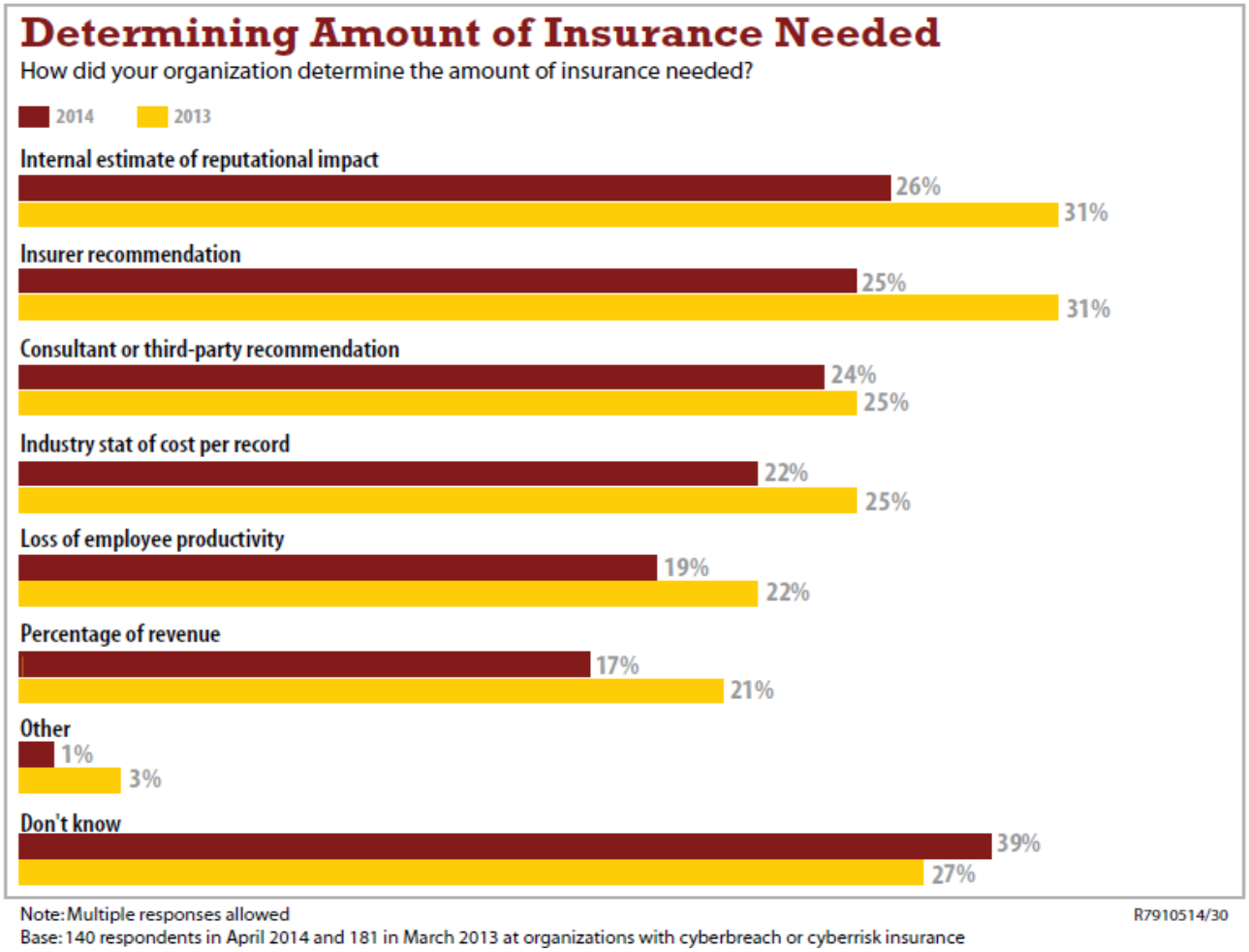
27% of small businesses

have insurance that would cover them in the event of a breach.

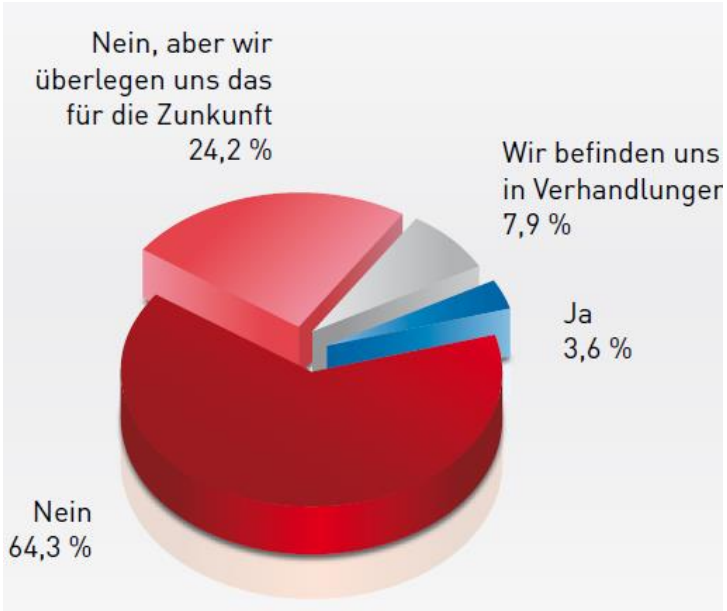
[PWC Information Security Breaches Survey, 2015]

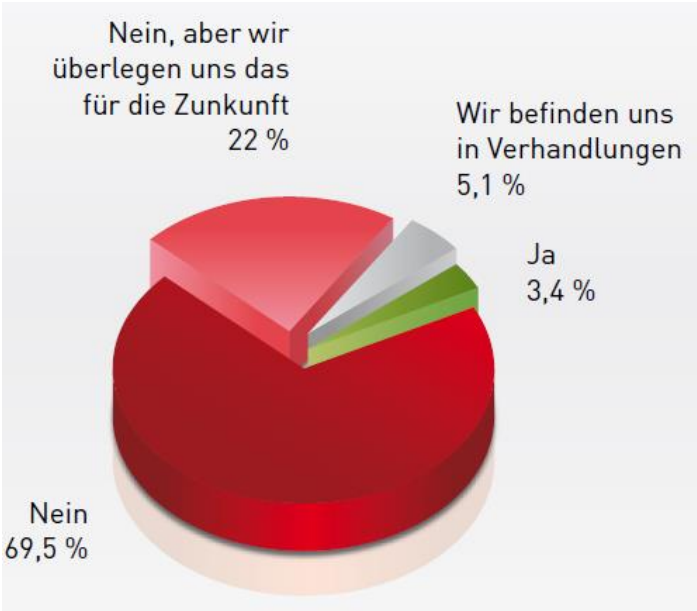
The Sizing Challenge

[Information Week Strategic Security Survey, 2014]



Considerations in Germany & Austria





[Corporate Trust: Studie Industriespionage 2014]

sbaPRIME: Staying Up To Date

Security Studies in a Nutshell

Bias in (Security) Surveys

General problems (Security) Surveys face & Factors reducing their validity…

… or …

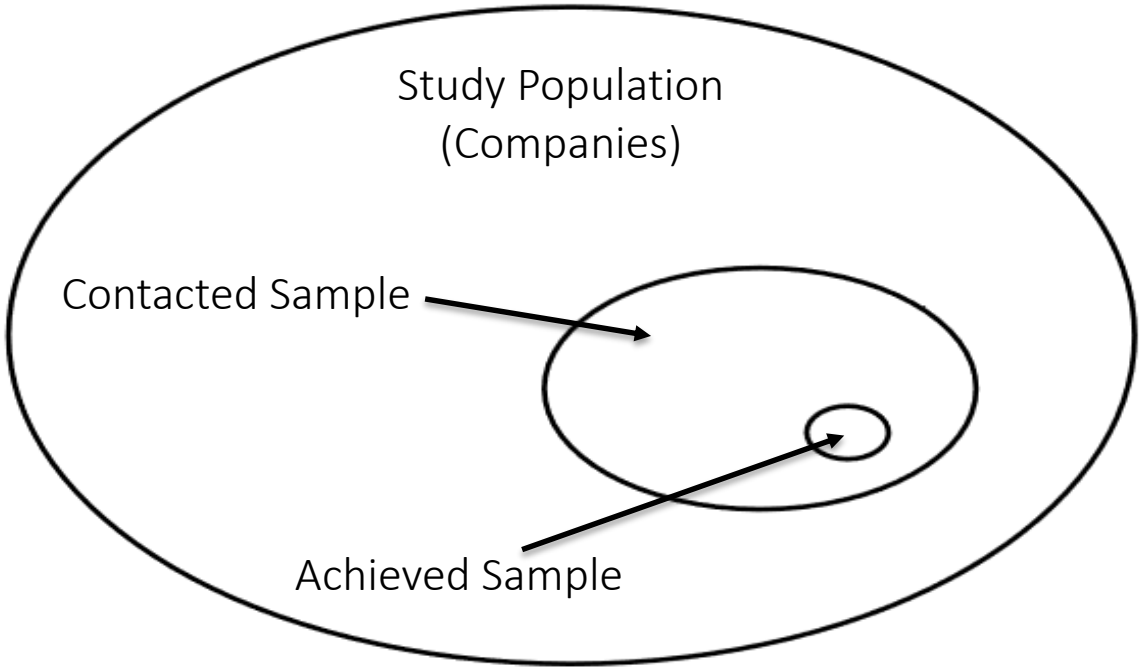
I only believe in statistics that I doctored myself

attributed to Winston S. Churchill

General problems (Security) Surveys face

What is Bias?

- **Bias** is a **systematic deviation** and **distortion** of **results**
- This leads to the **sample** itself and the **results of the study not being representative** of the (study) **population.**

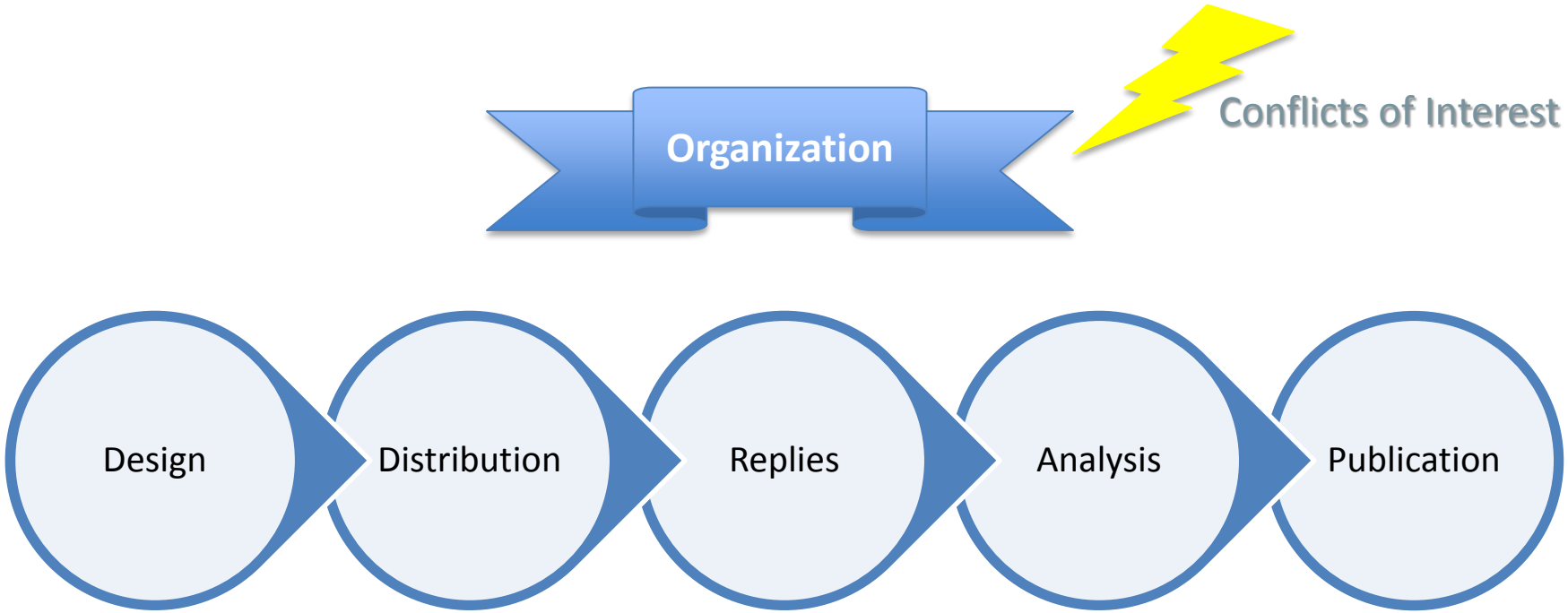


General problems (Security) Surveys face
Streetlight Effect

http://discovermagazine.com/2010/jul-aug/29-why-scientific-studies-often-wrong-streetlight-effect

General problems (Security) Surveys face

Survey Phases



General problems (Security) Surveys face
Conflicts of Interest

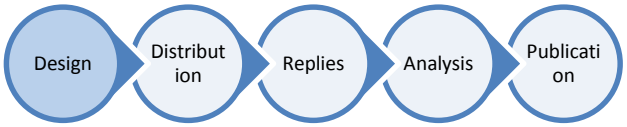
sbaPRIME

- Hardly **independent surveys** (Universities, independent Researchers etc.)
- **Conflicts of Interest**
  - Most Surveys & Reports by Security Vendors, ISPs, Incident Response Firms, Consulting Companies, Law enforcement
- Their **economic interest** is obvious:
  - The **larger the threat seems** the **more important it is to buy their software** or ask for their services
- Their **business relies on convincing companies** that **they are at risk**
  - Not that they (at least some of them) are not at risk but **risk should be presented realistically** and **not exaggerated**.
  - In order to focus activities & spending appropriately valid & trustworthy numbers are necessary.

http://www.propublica.org/article/does-cybercrime-really-cost-1-trillion
http://research.microsoft.com/apps/pubs/?id=217438

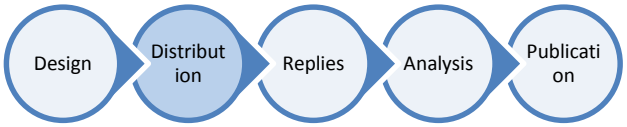
General problems (Security) Surveys face

Design Phase



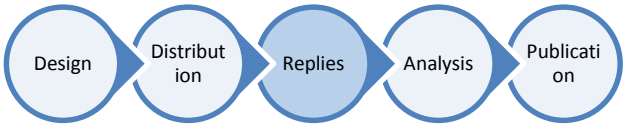
- **Methodology**
  - Survey design, Sample selection, randomization, Hypotheses etc.
- **Expectations** of the author & organization
  - Do heavily influence the results of the survey, maybe even don‘t publish „unwanted“ results (Publication Bias)
- **Formulation** of Question
  - Not carefully designed questions may lead to **distorted responses**
- **Lack of Definitions**
  - No clear definitions of important terms → respondents giving **wrong answers**, no **comparability** of results of different surveys

General problems (Security) Surveys face
Distribution Phase



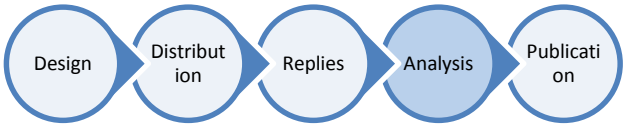
- **Sample Size**
  - if too small **not representative** & small **differences can‘t be identified** - sample size alone doesn‘t lead to representativeness
- Sample Quality
  - Sample not being representative of the population
- **Sample Composition** in **comparisons**
  - When comparing results (years, countries, groups) the **different sample composition** can **lead to wrong assumptions**
  - e.g. in Swiss sample more companies with an ISMS than in Austria, in the following year less SME & more huge companies
  - even **harder to compare results of different surveys**

General problems (Security) Surveys face
Reply Phase



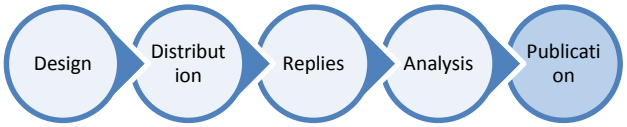
- Non Response & Self Selection Bias
  - Answers of respondents differ from the potential answers of those who did not answer, e.g. Respondents most likely have a higher security awareness & posture than typical companies
- Over confidence
  - Overestimate own security posture, e.g. 93% of the U.S. and 69% of the Swedish drivers believe themselves to be in the top 50%
- Reliance on self assessment by respondents also leads to
  - Misconception/False Answers
  - Lies
  - Social Desirability Response - Tendency to answer questions in a manner that will be viewed favorably by others, e.g. deny drug use, company not admitting lacking basic security measures

General problems (Security) Surveys face
Analysis Phase



- **Confirmation Bias**
  - **Focus on information** which **confirms one's beliefs** or hypotheses. Give disproportionately less attention to information that contradicts it. **We all suffer from it every day!**
- No **weighting**
  - Weight sample so that it resembles the study population
- **Outliers handling?**
- **Correlation vs. Causality** (also a Problem in Big Data Analysis)
  - **"Storks & Births",** "Ice-Cream consumption & sunburns"
- Description of **Methodology** & **Elaboration** on **Limitations**?

General problems (Security) Surveys face
Publication Phase



- **Exploitation** for **Marketing purposes** & FUD mongering
  - **Sensationalism**, very widespread, **Draw attention to some (high) numbers** which imply the situation is bad, don‘t describe **context of numbers,** lack of objectivity & thorough methodology
  - e.g. Raw number of malware samples, Users trading password for chocolate bar, Cost of Cybercrime…
- No **peer review**
  - Contrary to publication in academic journals **no formal system of oversight** for studies published by industry
- **Reproducibility**?
  - Ensure and verify correctness of results & findings, very important topic which **gains far too few attention** (in science in general!)

General problems (Security) Surveys face
Cost of Cybercrime - One Example

- *….stole intellectual property from businesses **worldwide** worth **up to $1 trillion**.* *– US President Obama, 2009 Cybersecurity speech*

- 1 Trillion estimate *very!* **inaccurate** & **not trustworthy**
  - Our assessment of the quality of cyber-crime surveys is harsh: they are so compromised and **biased** that **no faith whatever can be placed in their findings**

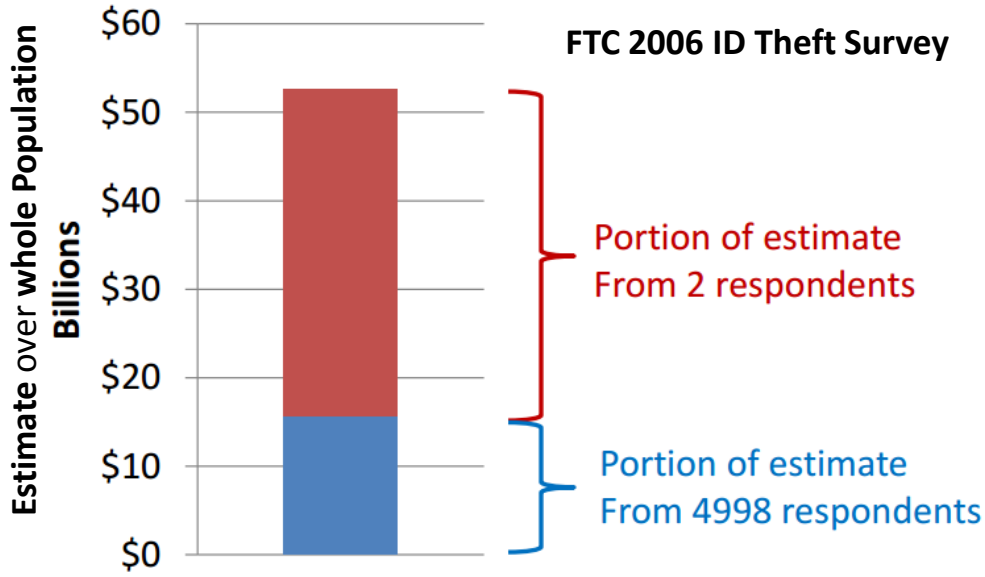
    Dinei Florencio & Cormac Herley, Microsoft Research
  - They all *[big commercial cybercrime surveys]* suffer from **major weaknesses**, which means the **data is worthless**, scientifically worthless. But it's very **valuable from a marketing perspective**

    Julie Ryan

http://www.propublica.org/article/does-cybercrime-really-cost-1-trillion
https://www.whitehouse.gov/the-press-office/remarks-president-securing-our-nations-cyber-infrastructure

General problems (Security) Surveys face
Cost of Cybercrime - Problems

- **Unverified claims** (self reporting), **Outliers & losses** (amount) **unevenly distributed** (heavy tail distribution)
  - Cyber Crime estimates appear to be largely the **answers of a handful of people** extrapolated to the whole population
  - A **single** individual who **claims** $50,000 losses is **enough to extrapolate a $10 billion loss** over the population.



http://research.microsoft.com/pubs/149886/SexLiesAndCyberCrimeSurveys_ITTC.pf

General problems (Security) Surveys face

sbaPRIME

Cost of Cybercrime - Problems

- **Basic problems** still remain
  - What is cybercrime?
  - How to for example measure worth of an SSN or IP?
  - Include costs for Recovery & Defense?
  - Under Reporting
  - Dark figure of breaches. Victims who don't know they suffered a breach
- Very **wide range of estimates** Cybercrime estimates
  - Everywhere from $560 million to $1 trillion

How do you even start to measure the monetary damages? **I would argue it is impossible**. I don't see how you can adequately come up with dollar figures.

Nick Akerman, Contributor to the McAfee report

Well, we all need information!

It‘s better to have some data than no data…

We **don‘t** have the **map for JFK airport** so the one for **Chicago must suffice**.
It is better to have some map than no map.

Nassim Nicholas Taleb, Der Schwarze Schwan

General problems (Security) Surveys face
Conclusion

- Many sources for errors, problems & bias
- **Some** problems & bias **hardly avoidable**

- What **you** can do
  - ***Don‘t be too trustful!***
  - **Always question methodology, results** & **intentions**
  - Think about **possible limitations**
  - Remain **skeptical, wary** and **questioning**

- **Let us help you assess** the **plausibility & credibility of Surveys!**
  - Development of a **systematic approach** and **criterions**
  - White paper: How to read (security) surveys

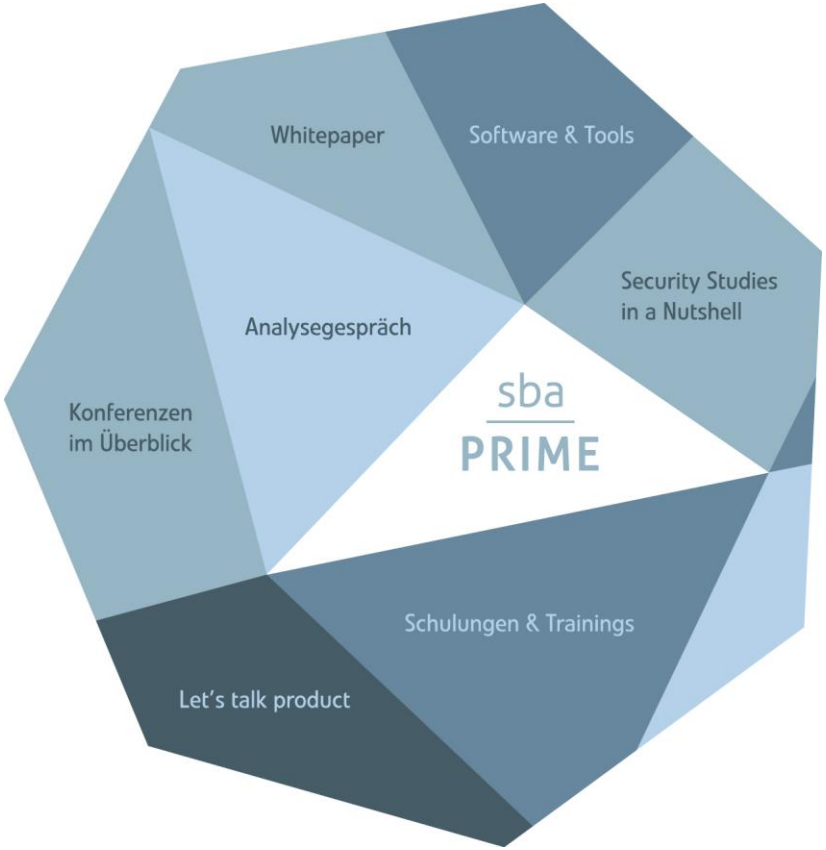
SECURITY STUDIES IN A NUTSHELL

Stefan Jakoubi & Philipp Reisinger

SBA Research gGmbH

Favoritenstraße 16, 1040 Vienna, Austria

{SJakoubi, PReisinger}@sba-research.org


Whitepaper
Software & Tools
Security Studies
in a Nutshell
Analysegespräch
sba
PRIME
Konferenzen
im Überblick
Schulungen & Trainings
Let's talk product

How to secure legacy systems

LET’S TURN IT OFF!

Legacy Systems

http://www.taroticallyspeaking.com/readings/framing-tarot-card-reading-questions/, 08.11.2015

Legacy Systems

„Infographic: Windows Server 2003 Migration: Are You Ready?“, Symantec
http://www.symantec.com/content/en/us/enterprise/fact_sheets/b-ws2003-eol-migration-infographic-ds.pdf

Legacy Systems

Clock ticking on Windows Server 2003 extended support timeline

The end of extended support for Windows Server 2003 is just under
manager says the average migration will take 200 days, so start thin
if you haven't already.

By James Sanders | August 1, 2014, 4:44 AM PST

Windows XP Is Still a Favorite Among Hackers

Microsoft no longer supports Windows XP, but it remains popular, and is a juicy target for cybercriminals.

By Mike Orcutt on October 15, 2014

...lassified Navy document, Microsoft applications affect "critical
...and control... ...based legacy systems, leaving them open
to potential cybersecu... ...ork to rid
themselves of these l...

According to an IDG ...
contract that would ...
entire length of the contract, the total will rea...

Use of Windows XP makes European ATMs vulnerable to malware attacks

By Loek Essers | Follow
IDG News Service | Apr 9, 2015 7:25 AM PT

RELATED

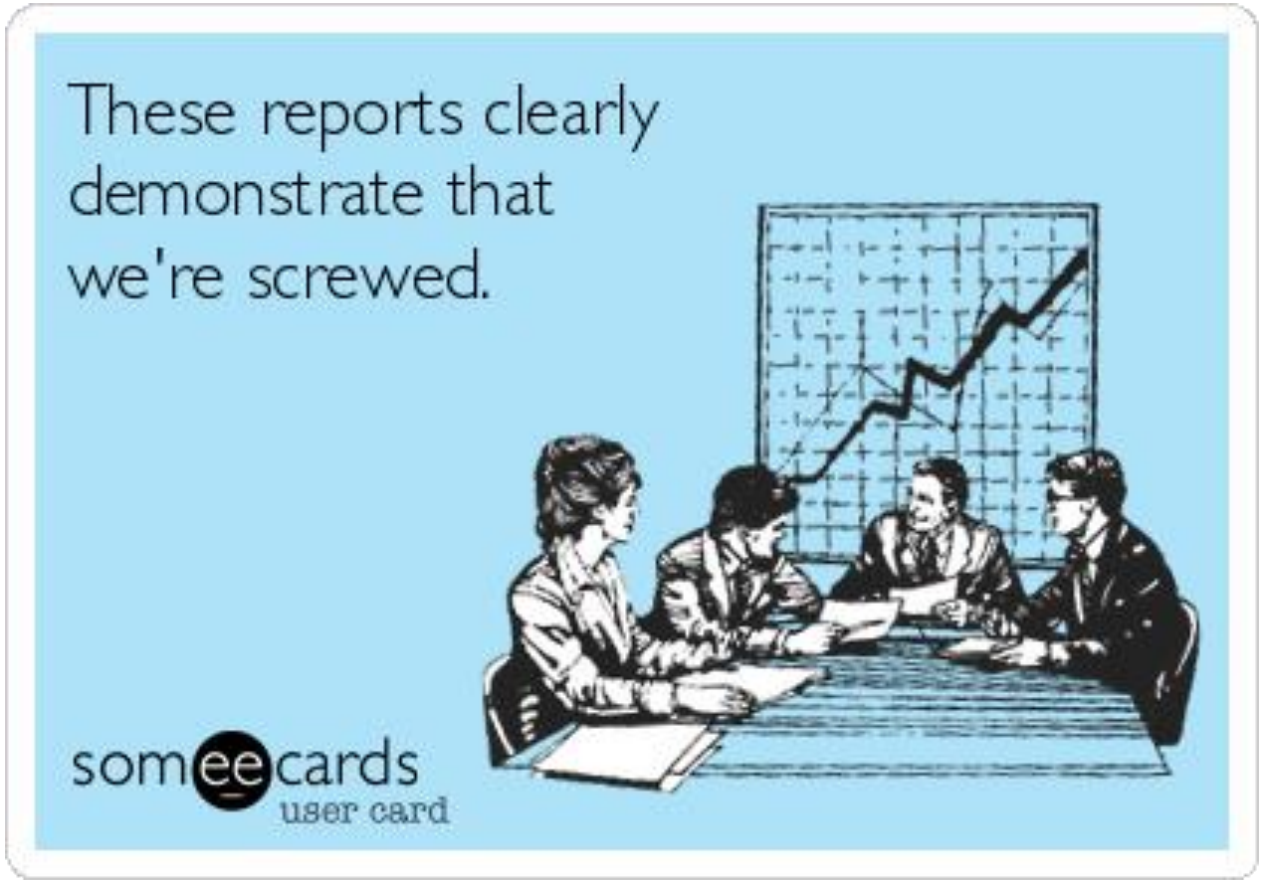
European banks see new ATM sl... attacks

Water utility companies using XP

Last year, Forbes reported at an alarming 75 percent of life-sustaining water utility companies were still operating using Windows XP. Numbers like that make this area vulnerable to cyber attacks. According to Matt Wells, general manager for automation software at GE Intelligent platforms, the utilities industry are slow to adopt new

Protecting Legacy Systems

- What now?

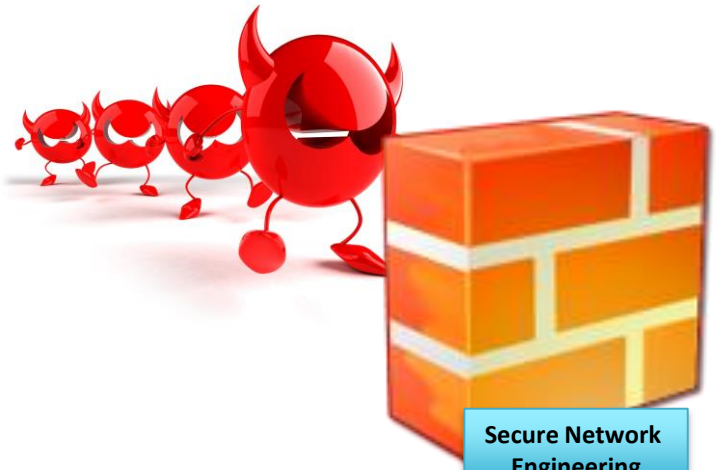


http://www.someecards.com/usercards/viewcard/these-reports-clearly-demonstrate-that-were-screwed-da5b9, 08.11.2015

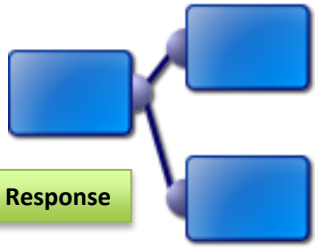
Protecting Legacy Systems

PROACTIVE

REACTIVE



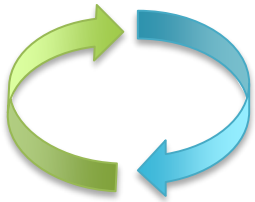
Secure Network Engineering



Incident Response

Continuous Monitoring

System Hardening



Data Protection

Data Recovery

Breach Detection and Prevention

System Virtualization

Continuous Risk Evaluation and Assessment

Protecting Legacy Systems

- For more details on legacy systems protection, have a look at our whitepaper

Isolation of Legacy Systems

-

A View on Security Concerns for Non-Isolated Legacy Systems

THANK YOU!

https://media.licdn.com/mpr/mpr/p/8/005/07c/0e0/2dc813d.jpg, 08.11.2015

WHITEPAPERS

Christoph Falta

SBA Research gGmbH
Favoritenstraße 16, 1040 Vienna, Austria
CFalta@sba-research.org


sba
PRIME

Security Fails 2015

...you breaching copyright, but you are also making your devices vulnerable to viruses.

How to always stay a step ahead of the cyber thieves

FROM PREVIOUS PAGE

than a laptop and phone, to create their own wifi network and lure unsuspecting users to join it. Once you do so, the criminal can then steal your personal information.

This means you should only use wifi networks that you recognise and trust. If in doubt, ask the owner of the cafe, restaurant or shop you are in. And if you're unsure, don't use wifi to connect to the internet — instead, use your device's mobile connection.

WHAT'S SAFE TO DOWNLOAD?

YOU may be aware that thieves try to infect computers with viruses. Often, these are spread via email, and are installed on computers when an unwary recipient clicks on an attachment. Do not download anything, or click on anything — whether in an email or a webpage — that looks suspicious.

Tablet and smartphone users should also be wary of apps they download. Although they should never have viruses, sometimes they have connections to other apps on your device, such as Twitter and Facebook, and unscrupulous software developers can use these connections to access your details.

DO I NEED VIRUS SOFTWARE?

THIS is a must — and ignore people who say you don't need such software on Apple products or on tablets — you do! In order to protect your data and your computer, it is worth installing antivirus software — such as Avira, which is free and available from the Play Store and Apple App Store — that runs constantly and checks that no hackers are trying to gain access to your device.

can crack your password on, say, Amazon, they will then try your online bank account using the same password.

HOW TO BANK ONLINE SAFELY

THERE'S no doubt that online ...

the conmen by remembering these steps:

1 CHECK that you have an 'https' connection when you login. Before you log in to your account, look to see if the bank's web address in the browser bar starts with 'http' or 'https'. That extra 's' stands for 'secure', and this is what you need to see. Sites that just begin with 'http' are not secure, and you shouldn't enter any private information into them.

2 LOOK for the padlock! All secure sites feature a padlock icon in the browser bar. If you click on the padlock, a window will pop up featuring a security certificate, which will show that the website's owner has been verified. If you do not see the padlock, under no circumstances log in.

3 CHECK the web address. This may seem obvious, but make sure you have entered your bank's web address correctly. Many criminals try to register site names that look very similar to the correct address, or sites that are spelled like real addresses, but with common typing errors.

Keep your details safe

AGAIN, this may seem like common sense, but do not share your log-in details with anybody. Neither should you write them down — especially not on a sticker attached to the screen of your laptop!

Check your bank account regularly

IDEALLY, you should log in to your bank account every day and have a look through all recent transactions.

In addition, if your bank offers it, subscribe to a text service that will send weekly or daily balances to your mobile phone.

HOW TO SHOP ONLINE SAFELY

SHOPPING online is a growing business. But it comes with a risk. How do you know if your credit card details are secure? Follow ... safe shopping:

Tech tip
Make the most of your broadband by buying a new, superfast router. If yours is over two years old, consider replacing it

MAKE THE INTERNET SAFE FOR YOUR ...

WE'VE all heard the ... around the dinner ... grandchildren findin... inappropriate on th... And we've also re... sionable youngst... online by the most... For parents, gra... the internet repr... How best to pr... yet at the sa... continue to dra... and social ben... its entertain... simple steps:

CHECK YOUR S...

THIS is you... are you... internet... includ... Yahoo!... descri...

AGENDA

1) Staunen
2) Schmunzeln
3) Schaudern
4) Betroffen sein
5) GOTO 1)

WAS IST HACKEN?

Falsche Annahmen ausnützen

Größeres Schloß ≠ besseres Schloß

Nie die Vordertüre verwenden

DAS WAR 2015 … DIE HIGHLIGHTS


1 GERÄT | 1 JAHR
INKLUSIVE
ANONYMOUS MASKE
CyberGhost 2015 VPN
ZUVERLÄSSIGER SCHUTZ VOR DATENSPIONEN & HACKERANGRIFFEN
NOTWENDIGE ERGÄNZUNG zum bestehenden VIREN- & FIREWALL-SCHUTZ
SATURN
2015
eset
SMART SECURITY
2015

0Days: Wenn sich der Antivirus gegen dich wendet…

sbaPRIME

- FireEye
- Avast
- Kasperski

SSL Interception – considered harmful

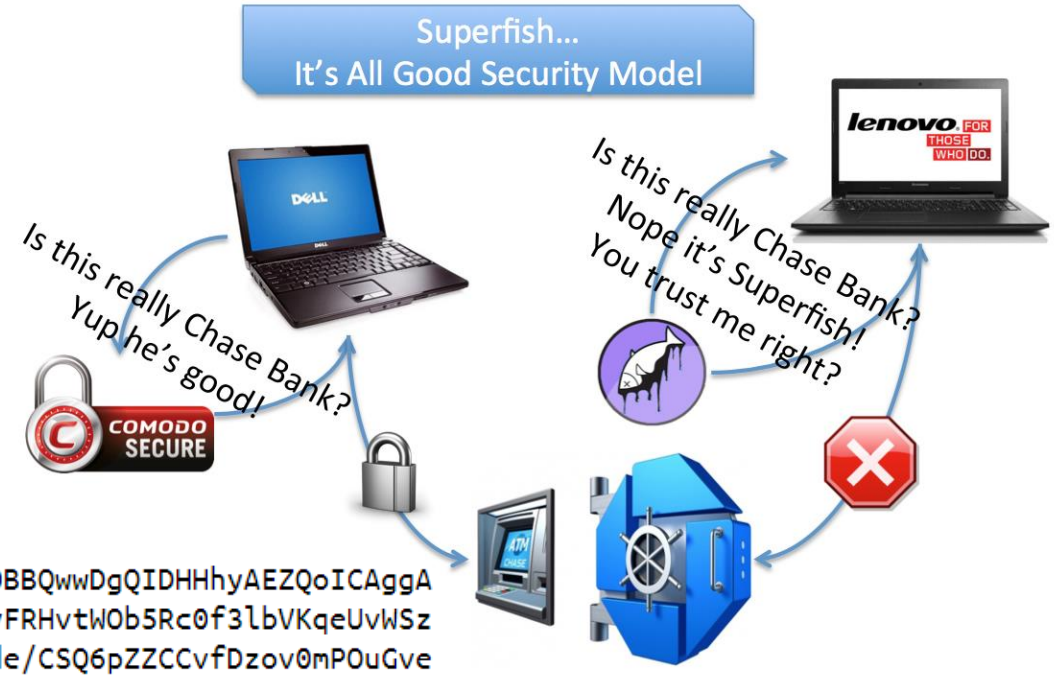
- “Superfish Visual Discovery” Adware

SSL Interception – considered harmful

- “Superfish Visual Discovery” ~~Adware~~
  Alternative Angebote zum Vorteil des Kunden
- Vorinstalliert auf
  Lenovo

SSL Interception – considered harmful

- “Superfish Visual Discovery” ~~Adware~~
  Alternative Angebote zum Vorteil des Kunden
- Vorinstalliert auf
  Lenovo




```
4844  pc2g&h
4845  IhvcD
4846  Unknown error
4847  equence
4848  operation
4849  SocketAsync
4850  -----BEGIN ENCRYPTED PRIVATE KEY-----
4851  MIICxjBABgkqhkiG9w0BBQ0wMzAbBgkqhkiG9w0BBQwwDgQIDHHhyAEZQoICAggA
4852  MBQGCCqGSIb3DQMHBAiHEg+MCYQ30ASCAoDEvGvFRHvtWOb5Rc0f3lbVKqeUvWSz
4853  xQn+rZELHnwb6baolmbFcsi6XkacVzL/EF7Ll4de/CSQ6pZZCCvfDzov0mPOuGve
4854  SAe7hbAcol7+JWVfzbnVTblPf0i7mwSvK61cKq7YfcKJ2os/uJGpeX9zraywWyFx
4855  f+EdTr348dOez8uHkURyY1cvSHsIdITALkChOonAYT68SVighTeB6xOCwfmsHx+X
4856  3Qbhom2YCIxfJiaAoz2/LndCpDaEfOrVrxXFOKXrIbmeDEyjDQj16AVni9uuaj7l
4857  NiO3zrrqxsfdVINPaAYRKQnS102jXqkH01z72c/MpMMC6dwZswF5V3R7RSXngyBn
```

Lenovo 2 – Das BIOS

- **Lenovos Service Engine**
- Im Bios verankert
- Installiert unbemerkt Lenovo Dienste nach
  - Diese Laden dann “Updates” aus dem Internet
  - Lassen sich austricksen, Beliebiges nachzuladen

Distribution Problems

- Was ist schlimmer als zu Manipulieren?

Distribution Problems

- Was ist schlimmer als zu Manipulieren?
- Den Beweiß dafür in hundertausend Produkte einzubauen

… für den USA Reisenden von heute…

Washington Post (Print 2014, Online 2015)

… noch in der selben Nacht …

https://github.com/Xyl2k/TSA-Travel-Sentry-master-keys

Plastik-Router Botnets

The Register®
Biting the hand that feeds IT

DATA CENTRE SOFTWARE NETWORKS SECURITY INFRASTRUCTURE BUSINESS HARDWARE SCIENCE

Security

Home routers co-opted into self-sustaining DDoS botnet

Resulting mess will

13 May 2015 at 18:19, John L

PC NEWS / OPINIONS / FEATURES / DEALS / HOW-TO / BUSINESS / V
ALL REVIEWS / LAPTOPS / TABLETS / PHONES / APPS / S

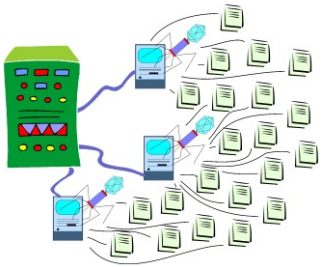
Home / Reviews / Networking / Security / Is Your Router a Botnet Zombie?

Is Your Router a Botnet Zombie

BY MAX EDDY MAY 14, 2015 COMMENTS

A newly-discovered global network of zombie routers has been used to launch DDOS at

0 SHARES



Security company Incapsula uncovered a massive botnet launch distributed denial of s (DDOS) attacks. But this botr made of infected computers. an army of zombie routers, p its master's bidding.

Incapsula observed traffic fro over the course of 111 days. time, it identified some 40,26 addresses used in the attack. infected machines appeared worldwide, coming from 1,600 Intern providers.

What's especially surprising about this botnet is that it wasn't bui some unique new attack. Incapsula discovered that the routers ir were all configured for remote management, meaning users (or a could discover them online and make changes. Nearly all the rou pre-set usernames and passwords, so taking control of them was trivial.

"Facilitating the infiltration, all of these under-secured routers are clustered in

News Cyber Attacks Vulnerabilities Malware Encryption Spying

The Hacker News™
Security in a serious way

+1,590,250 230,550 763,355

cyber security degree online

Routers TCP 32764 Backdoor Vulnerability Secretly Re-Activated Again

Sunday, April 20, 2014 Swati Khandelwal

Popular Stories


How to Weaponize your Cat to Hack Neighbours' Wi-Fi Passwords


This Secure Operating System Can Protect You Even if You Get Hacked


How Amazon Employee bought 'Google.com' Domain for Only $12 from Google


AdBlock Extension has been Sold to an 'Unknown Buyer'


Incredible! Someone Just Hacked 10,000 Routers to Make them More Secure


New Attack Targeting Microsoft Outlook Web App (OWA) to Steal Email Passwords


British Intelligence Agency


Replace With a $38 Tablet


25 Cool Things You Didn't Know Chrome Could Do

Plastik-Router Botnets

Malware implants on Cisco routers revealed to be more widespread

Cybersecurity for the planet Credit: Gerd Altmann / Pixabay

Researchers detected 200 Cisco routers with malicious firmware in 31 countries, with the U.S. having the largest number of potentially infected routers

By Lucian Constantin | Follow
IDG News Service | Sep 21, 2015

COMMENTS

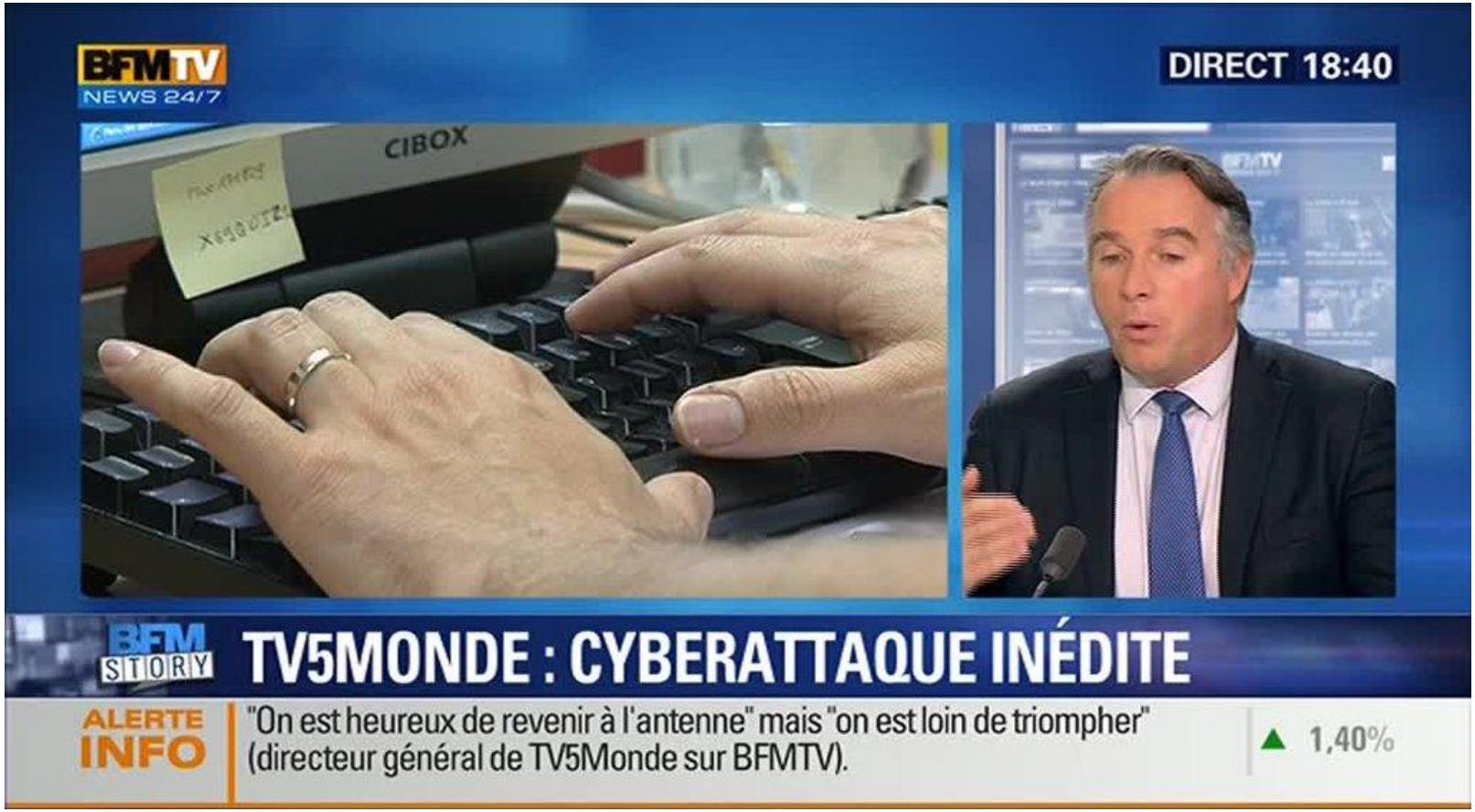
Attackers have installed malicious firmware on nearly 200 Cisco routers used by businesses from over 30 countries, according to Internet scans performed by cyber crime

TV5 /* April 2015 */

Password Policy bei TV5

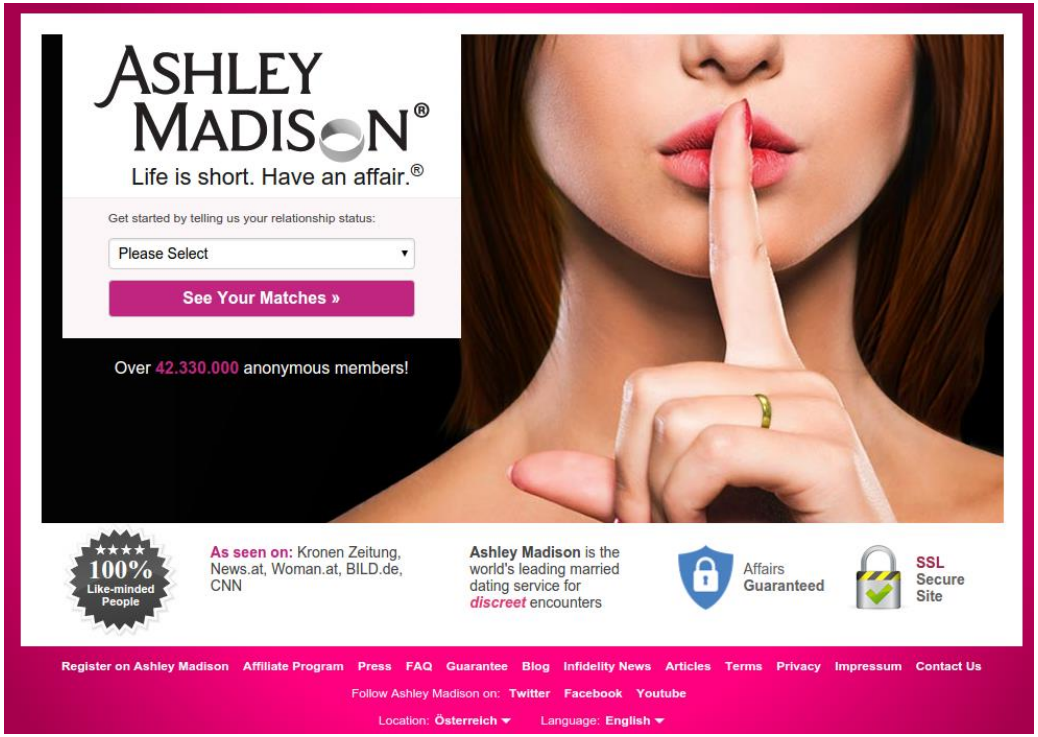
lemotdepassedeyoutube
~ „dasyoutubepasswort“

Mehr Passwörter bei TV5



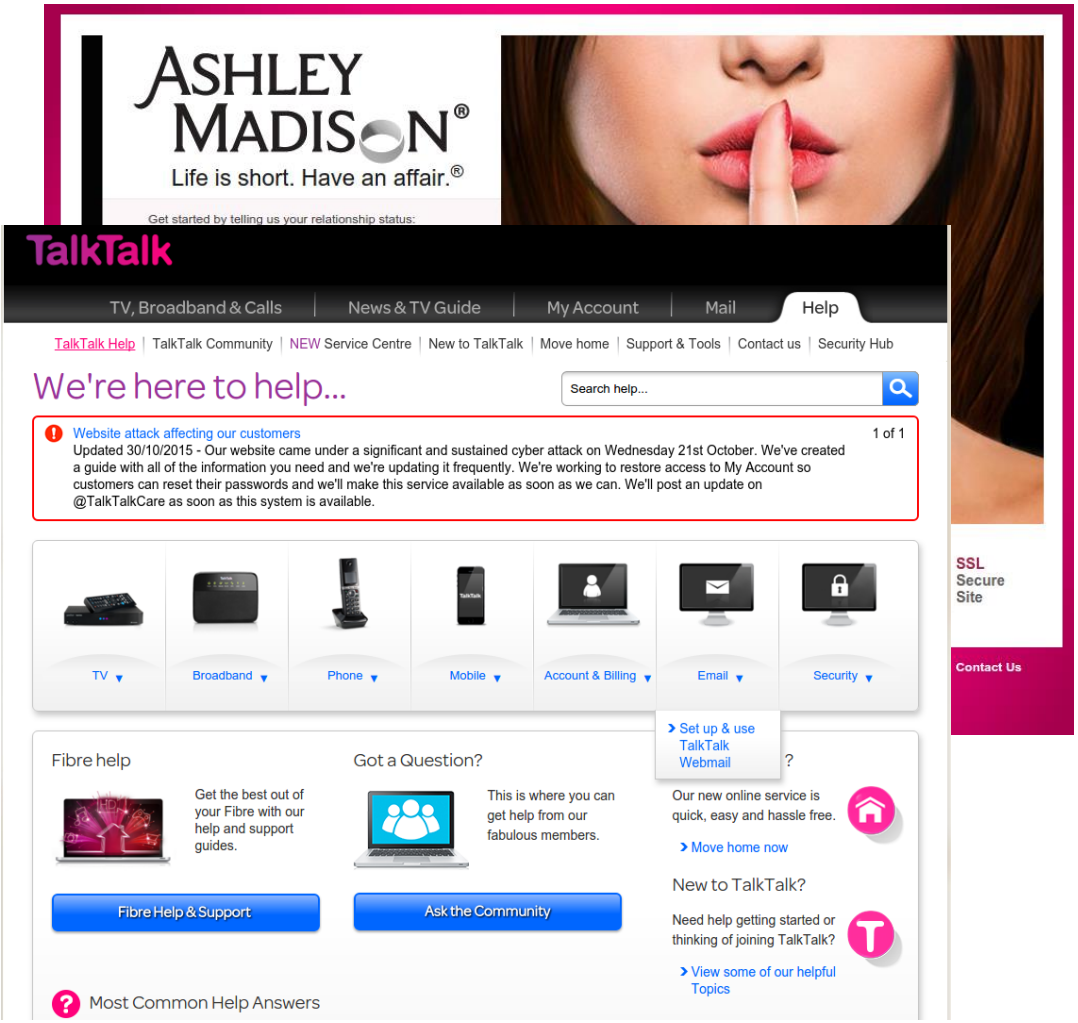
Passwörter Storage…

- Ashley Madison



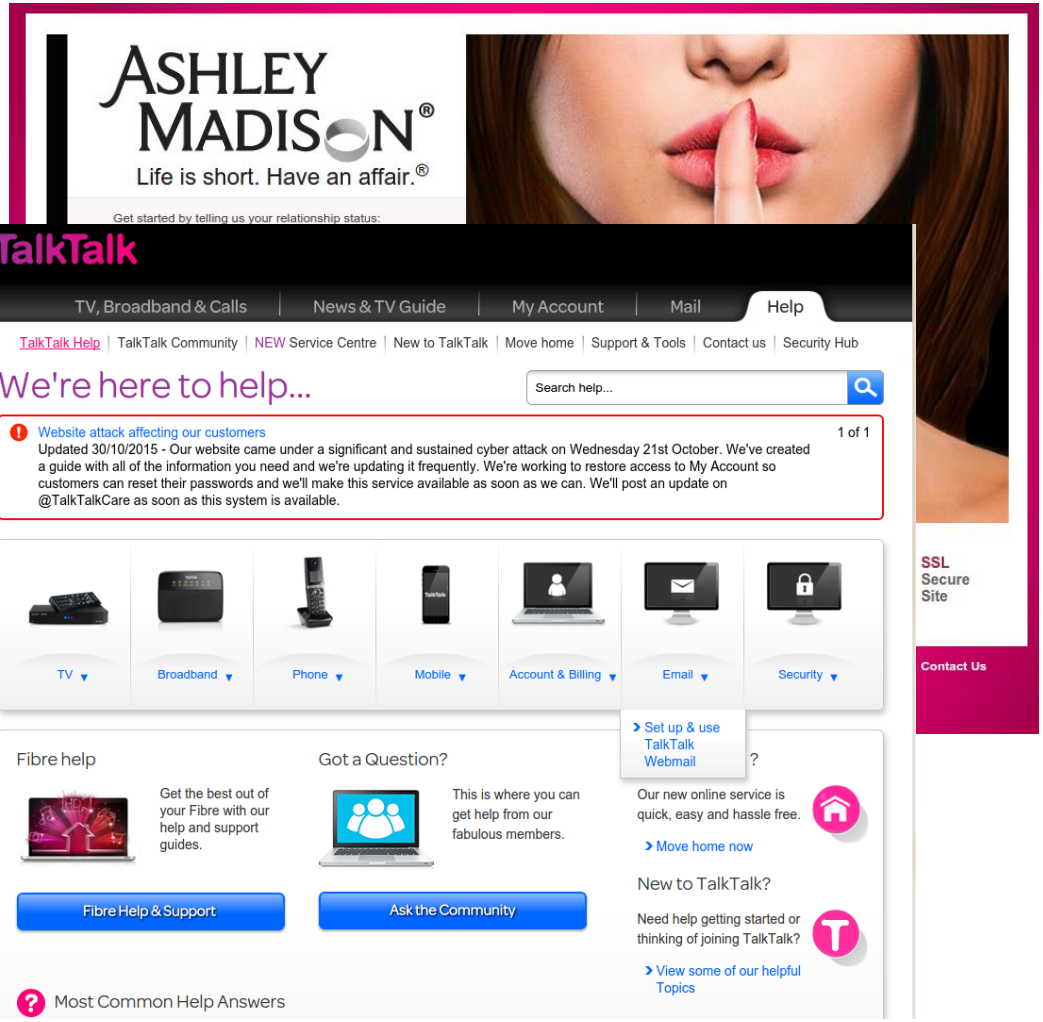
Passwörter Storage…

- Ashley Madison
- Talk Talk

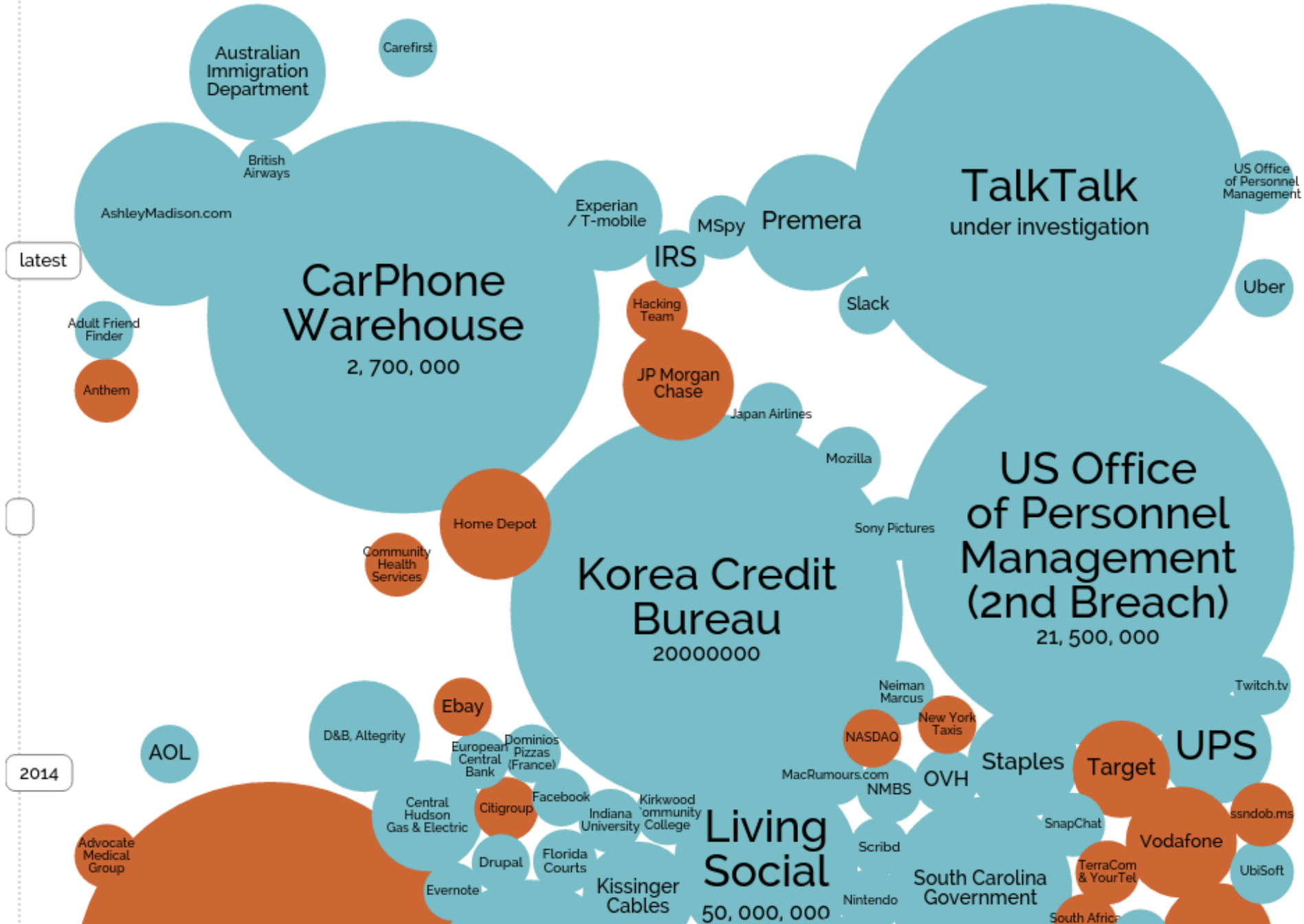


Passwörter Storage…

- Ashley Madison
- Talk Talk
- US Office of Personnel Mgnt.
- US Office of Personnel Mgnt.



http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/

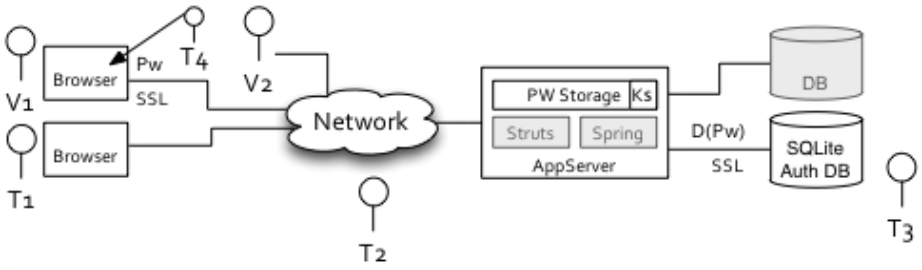


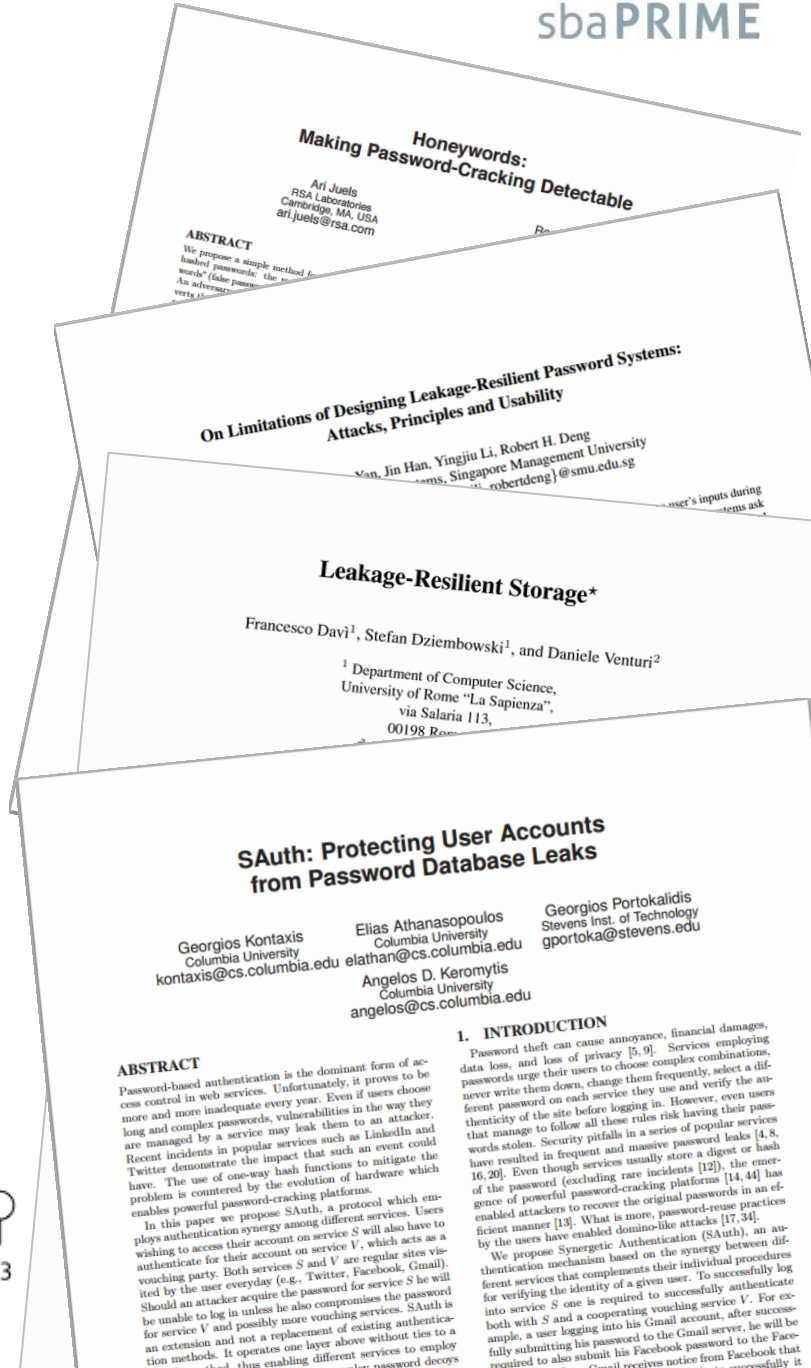

Someone figured-out my
PASSWORD
Now I have to rename my dog!
Use strong passwords
A simple password, such as your pet's name, is not sufficient protection. Hackers systematically check every possible word to decipher passwords in no time.
NETSCOUT.
Help protect our information assets.

Conclusio

Password Research

- Secure storage
- Leak proof storage
- Design for failure
- Honey-Passwords
- Usable Security
- Policies





Honeywords:
Making Password-Cracking Detectable

Ari Juels
RSA Laboratories
Cambridge, MA, USA
ari.juels@rsa.com

ABSTRACT

On Limitations of Designing Leakage-Resilient Password Systems:
Attacks, Principles and Usability

Jin Han, Yingjiu Li, Robert H. Deng
Singapore Management University
{robertdeng}@smu.edu.sg

Leakage-Resilient Storage*

Francesco Davì[1], Stefan Dziembowski[1], and Daniele Venturi[2]

[1] Department of Computer Science,
University of Rome "La Sapienza",
via Salaria 113,

SAuth: Protecting User Accounts
from Password Database Leaks

Georgios Kontaxis
Columbia University
kontaxis@cs.columbia.edu

Elias Athanasopoulos
Columbia University
elathan@cs.columbia.edu

Georgios Portokalidis
Stevens Inst. of Technology
gportoka@stevens.edu

Angelos D. Keromytis
Columbia University
angelos@cs.columbia.edu

ABSTRACT

1. INTRODUCTION

KONFERENZEN IM ÜBERBLICK

Adrian Dabrowski

SBA Research gGmbH
Favoritenstraße 16, 1040 Vienna, Austria
ADabrowski@sba-research.org


sba
PRIME