Data Breaches, Data Leaks, Web Defacements: why secure coding is important.

Raoul «Nobody» Chiesa

Founder, President, Security Brokers

4TH SOFTWARE ENGINEERING FOR DEFENSE APPLICATIONS CONFERENCE

The speaker

- President, Founder, **The Security Brokers**
- Principal, **CyberDefcon Ltd.**
- Independent Special Senior Advisor on Cybercrime @ **UNICRI**
  (United Nations Interregional Crime & Justice Research Institute)
- Former PSG Member, **ENISA** (Permanent Stakeholders Group @ European Union Network & Information Security Agency)
- Founder, @ **CLUSIT** (Italian Information Security Association)
- Steering Committee, **AIP/OPSI**, Privacy & Security Observatory
- Board of Directors, **ISECOM**
- Board of Directors, **OWASP** Italian Chapter
- Cultural Attachè. Scientific Committee, **APWG** European Chapter
- **Supporter at various security communities**

The company

We deal with **extremely interesting, niche topics**, giving our strong know-hows gained from **+20 years of field experience** and from our **+30 experts**, very well known all over the world in the'**Information Security** and **Cyber Intelligence** markets.

Our **Key Areas** of services can be resumed as:

- ✓ **Vertical Professional Security Trainings & Coaching**
- ✓ **Proactive Security**
  - With a deep specialization on TLC & Mobile, SCADA & IA, Space & Air, e-health, […]
- ✓ **Post-Incident**
- ✓ **Cyber Security Strategic Consulting** (Technical, Legal, Compliance, PR, Strategy)
  - On-demand «Ninja Teams»
- ✓ **Psychological, Social and Behavioural aspects** (applied to cyber environments)
- ✓ **Cybercrime Intelligence**
  - Botnet takeovers, takedowns, Cybercriminals bounting, Cyber Intelligence Reports, Technical & Operational support towards CERTs and LEAs/LEOs,[…]
- ✓ **Information Warfare & Cyber War** (only for MoDs)
  - 0-day and Exploits – Digital Weapons

Abstract

- This presentation will **provide a "big picture"** towards those **main threats** linked with information theft and leaks, and web defacements, along with those **consequent impacts on organizations**.

- The **second part** of the talk will **focus on the importance of the so-called "Secure Programming"** and on those **average mistakes** that pop up when **running security testings** and **advanced Penetration Testing** activities **towards web applications**.

SALLY BEAUTY SUPPLY
viator
amazon Try Prime
KOREA.net Gateway to Kore
UNIVERSITY OF MARYLAND
ebay
DQ
TOKYO ELECTRIC POWER COMPANY
BARTELL HOTELS
WORKSOURCE OREGON
J.P.Morgan
Heartland
GEORGE MASON UNIVERSITY
Yandy.com
HARBOR FREIGHT TOOLS
Quality Tools at Ridiculously Low Prices
kmart
SHOP YOUR WAY
Michaels
Schnucks
Cyberswim
SAUSALITO YACHT CLUB
abc
Neiman Marcus
MONTANA DPHHS
Healthy People. Healthy Communities.
NORTH DAKOTA UNIVERSITY SYSTEM
ARRL CENTENNIAL
JIMMY JOHN'S GOURMET SANDWICHES
Albertsons
Experian A world of insight
SUPERVALU
sears SHOP YOUR WAY
PADDYPOWER GAMES
COUNTY OF LOS ANGELES CALIFORNIA
MORRISONS
Central Utah Clinic PC Your Health, Your Choice.SM
TJX THE TJX COMPANIES, INC.
salesforce
THE HOME DEPOT
RT
Goodwill Industries International, Inc.
Bashas' Your Arizona hometown grocer
nomorerack Everything You Love, For Less
P.F. CHANG'S
CHS Community Health Systems
kt
StubHub!
Google
at&t
Benesse
Benesse Holdings, Inc.
CHASE


What Do They Have In Common?

They All Did Not Even Had a Clue What Hit Them

Despite Having Spent Millions on All The "Best" Security Products, Software & Consultants

Why Not?

Because They Didn't Know What They Didn't Know

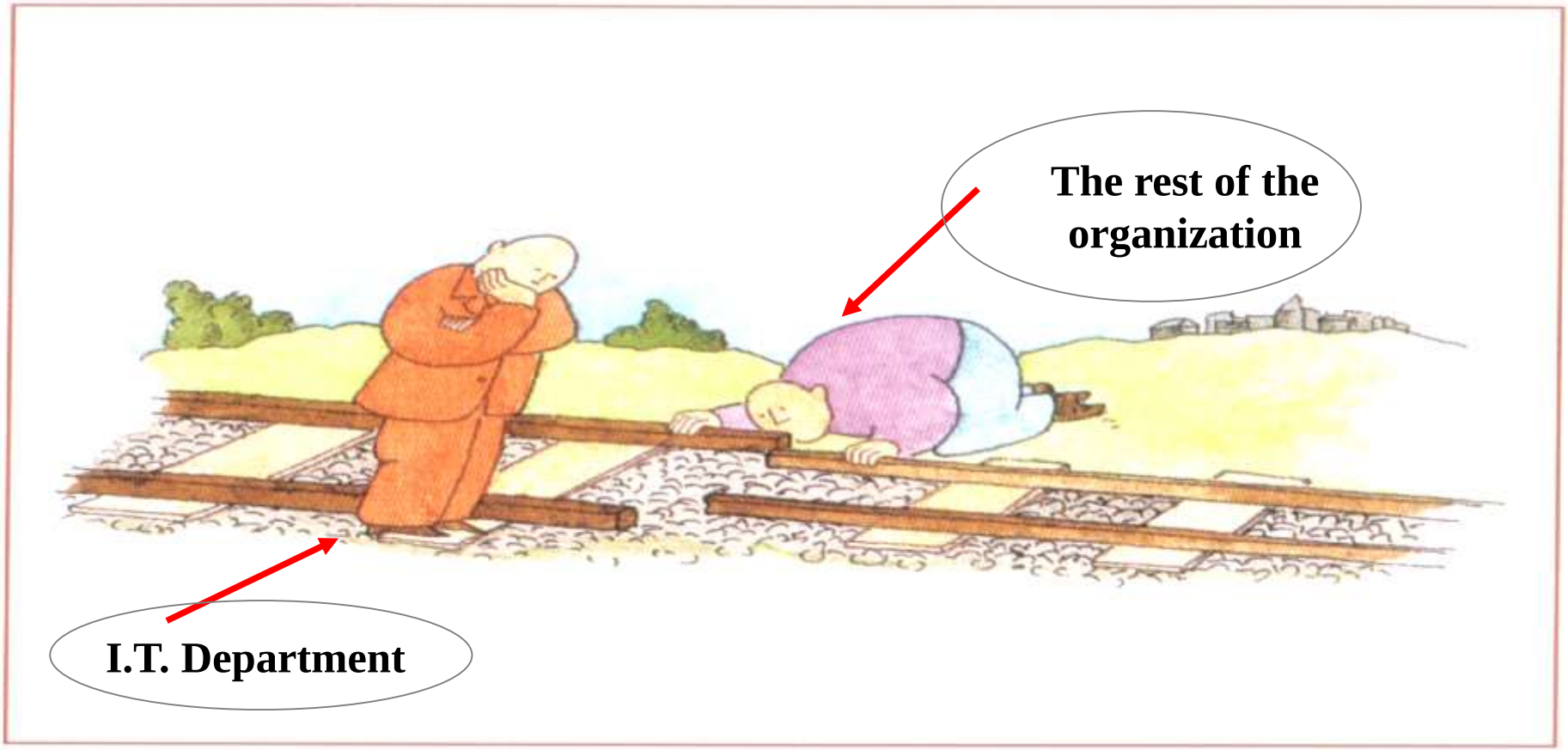
Because a Hacker only needs to Detect a Single Weak Spot where to stick the needle in.

Hackers Prefer Needling!!

Where on The Other Hand, You Need to Be Aware of EVERY New Spot a Hacker May possibly Stick A Needle ANYWHERE in YOUR Organisation ANYTIME.

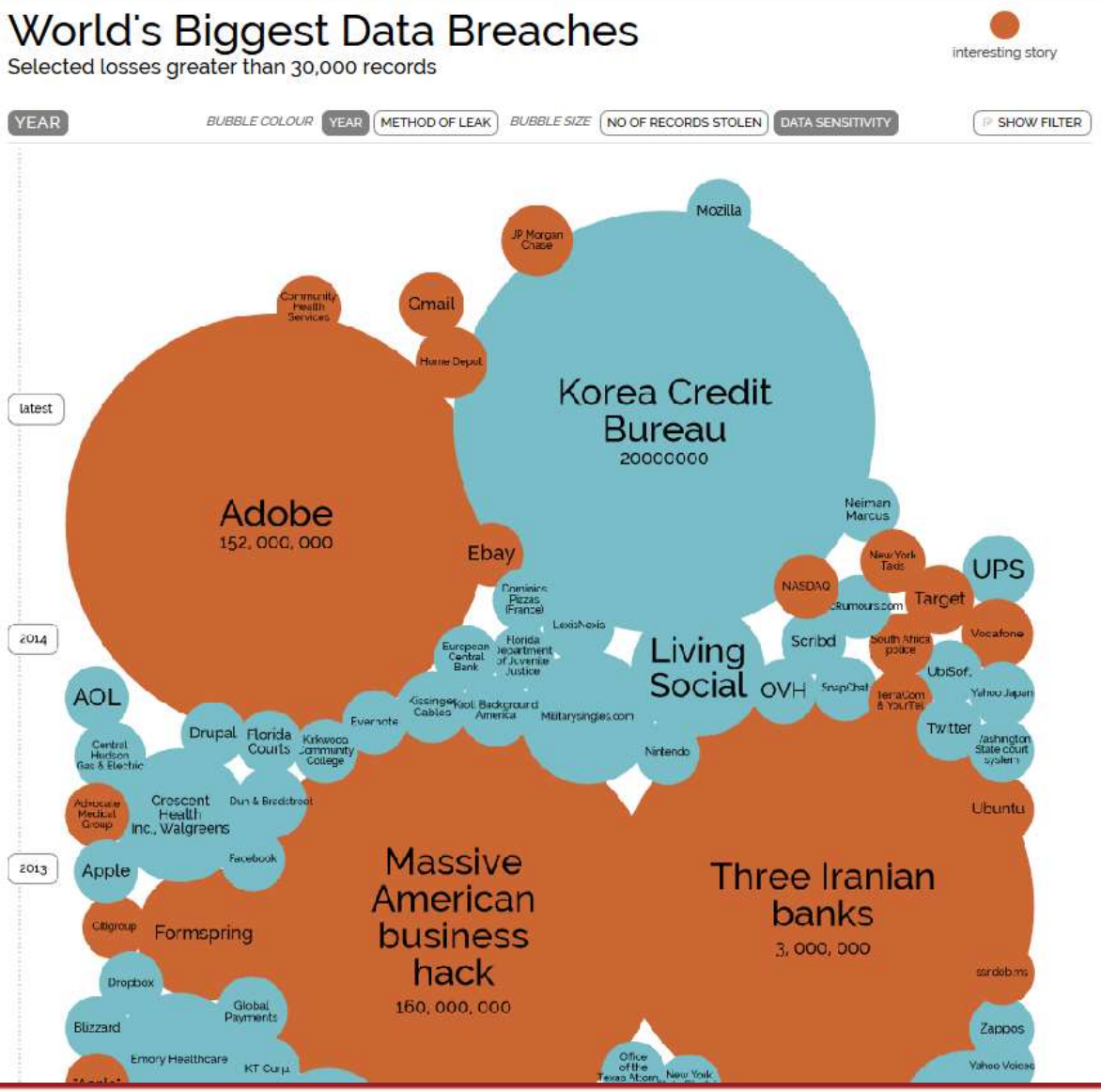
And You Need that Knowledge 24x7, With as Much Time as Possible to Take Preventive Action.
BEFORE you get hit!!

«Houston, we've got a problem…»



Know Your Attack Surface and be Timely Alerted on Relevant Threats and Risks, Well Ahead of a Possible Attack

Data Breach



Filter by...

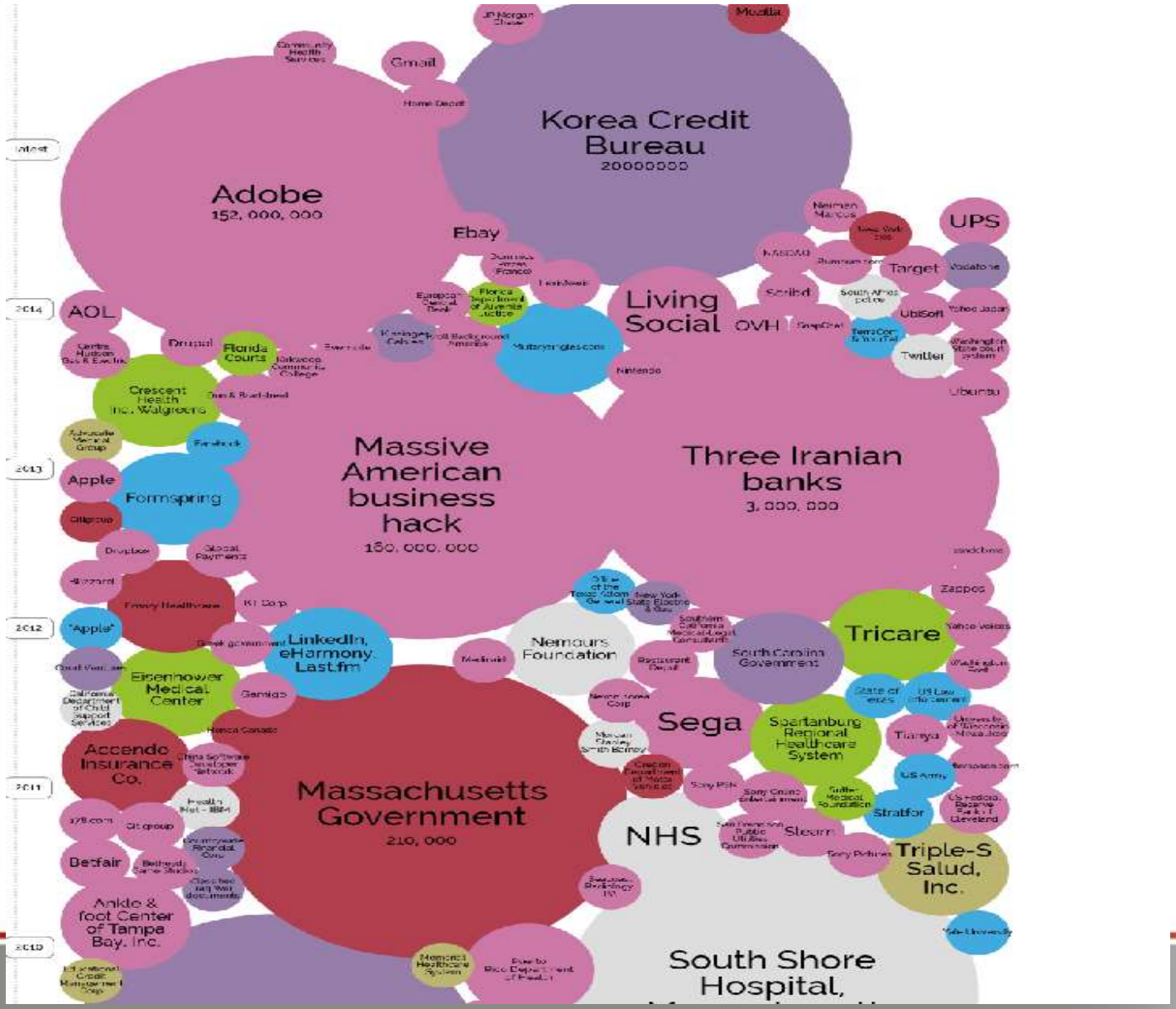
ORGANISATION

- [x] all
- [ ] academic
- [ ] energy
- [ ] financial
- [ ] gaming
- [ ] government
- [ ] healthcare
- [ ] media
- [ ] military
- [ ] retail
- [ ] tech
- [ ] telecoms
- [ ] transport
- [ ] web

METHOD OF LEAK

- [x] all
- [ ] accidentally published
- [ ] hacked
- [ ] inside job
- [ ] lost / stolen computer
- [ ] lost / stolen media
- [ ] poor security

Ops… it wasn't complete!



Filter by...

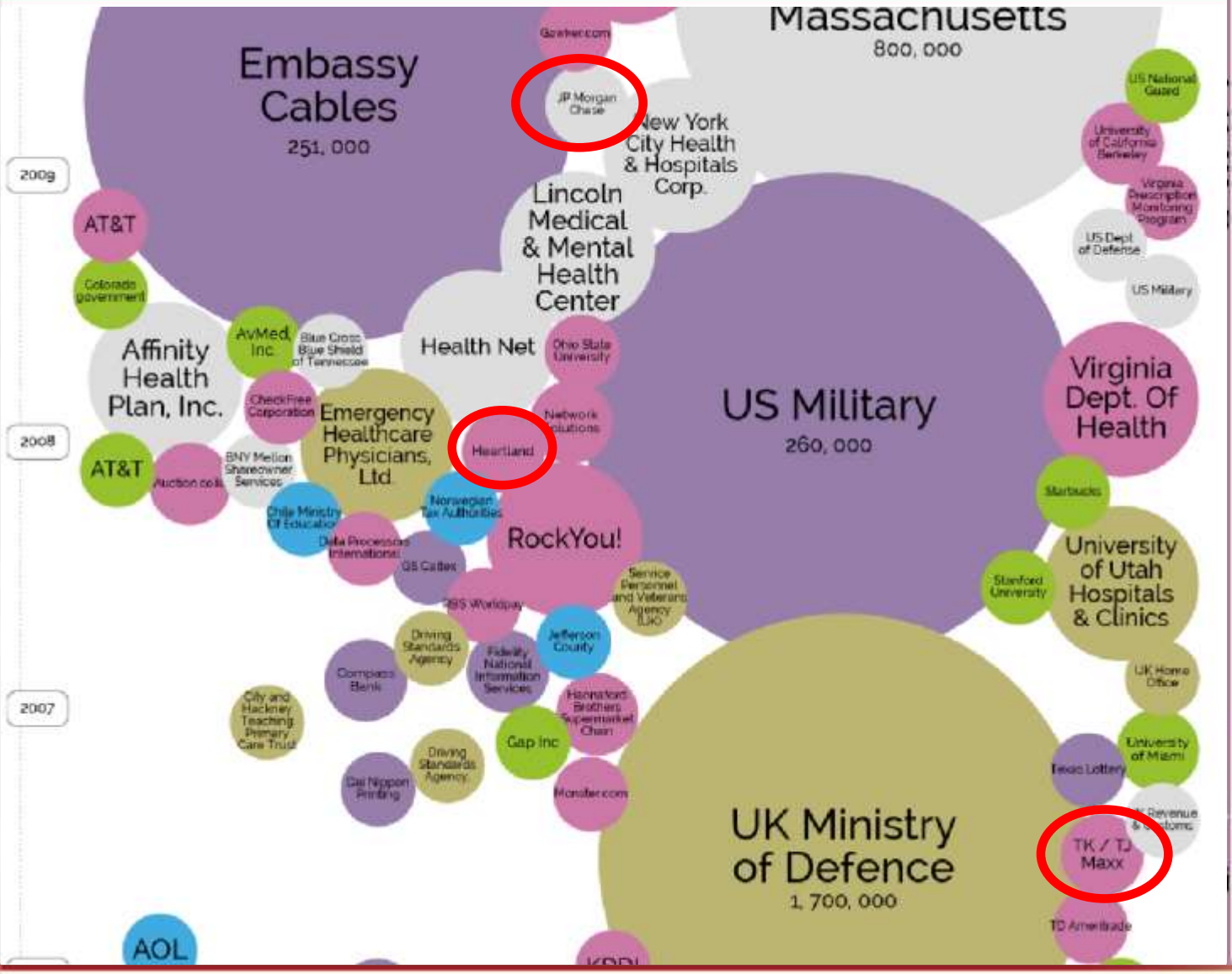
ORGANISATION

- all
- academic
- energy
- financial
- gaming
- government
- healthcare
- media
- military
- retail
- tech
- telecoms
- transport
- web

METHOD OF LEAK

- all
- accidentally published
- hacked
- inside job
- lost / stolen computer
- lost / stolen media
- poor security

Ops… it wasn't complete!



Filter by...

ORGANISATION

- all
- academic
- energy
- financial
- gaming
- government
- healthcare
- media
- military
- retail
- tech
- telecoms
- transport
- web

METHOD OF LEAK

- all
- accidentally published
- hacked
- inside job
- lost / stolen computer
- lost / stolen media
- poor security

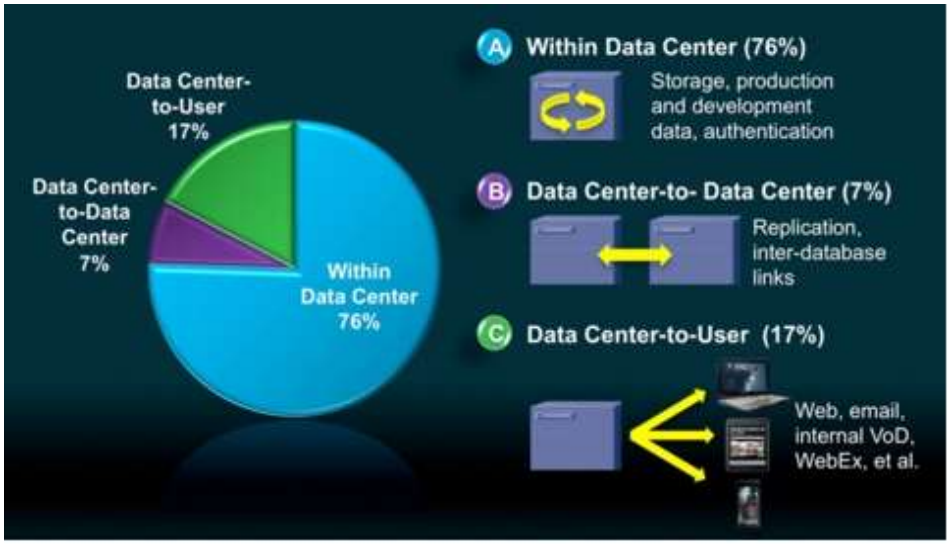
Ops… it wasn't complete!

Our analysis

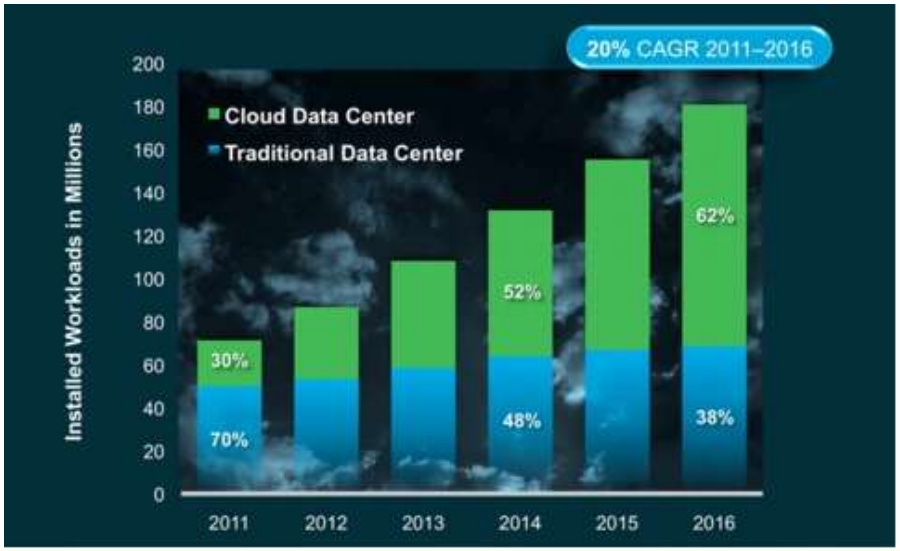
- The «world's biggest data breaches» have been **that many**, since 2004 'till today, they **can't even fit on a single page** ☹
- Further details here::
  - http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/
- We're speaking about a endless **escalation**
- **No one is excluded from this. Not anymore**
  - Also, **we depend too much on M2M**
- **Information = Power**. Which can be transformed in **money**, very quickly
  - The **damage caused by such breaches** is often difficult to calculate
  - **Operative**, **Business**, **Image**, **Economical damages** (**money refundings** to Customers**, fines** from Authorities).

M2M, Cloud and «automatic» connections

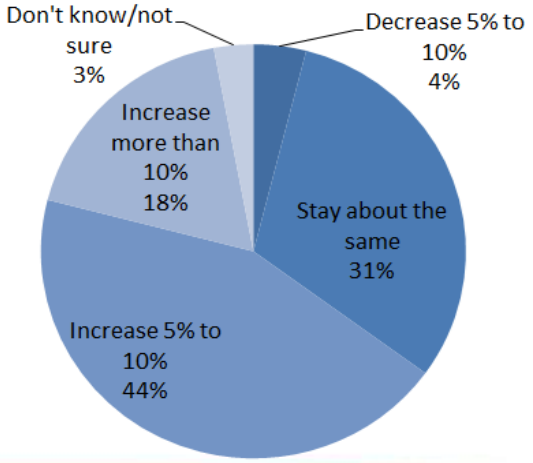
83% of Data Center traffic is M2M



Cloud services bring more M2M automation



Business and operational process automation drives most machine-to-machine transactions. How do you expect your organization's machine-to-machine (M2M) transactions and processes will change in the next 12 months?



Our analysis /2

Along with my team we **analyzied all of these data breaches**.

Key drivers to the **success of the attackers** can be resumed as

- **Lack of professionally-run Security Testings** (penetration test, ethical hacking, compliance check).
- **Lack of segregation** on **internal networks**.
- **Missing for a correct, centralized management** of **SSH keys**, both **external and internal ones.**
- **Missing of tools** for **Data Leak Prevention (DLP)** on **encrypted connections (SSH tunnels).**
- **Missing of the right sources for Cyber Intelligence.**
- **Lack of internal awareness.**
- **Lack or total miss of tools, methodolgoies and trainings on Digital Forensics.**
- **POOR PROGRAMMING / Lack of Secure Coding**

Mistakes when writing code

Vulnerability	Impact	Description
V-001 SQL Injection	The attacker can run arbitrary queries on the application DB, and potentially compromise it.	User's input is not correctly sanitized and it's inserted into a SQL query.
V-002 Weak password hashing algorithm	The attacker which has already obtained the password's hash values, could obtain clear-text passwords in a very quick timing, using commonly available techniques.	Passwords are stored with easy-to-decrypt algorithms and obsolete ones.
V-003 Weak Oracle passwords	Oracle users are activated with weak passwords, same as the username, or with default values.	Passwords of different Oracle users have not been changed, rather are obvious and easy-to-guess, or easy to crack (decrypt).
V-004 Excessive database user grants	In the scenario an attacker is able to execute commands on the DB through the web application, the user's privileges of the user assigned to the application are (too) high, allowing the attacker to run major damages from his actions.	The user which uses the DB has too high privileges, too much ahead of the standard instructions SELECT, INSERT, DELETE and UPDATE, which are needed by the application itself in order to work.
V-005 Multiple Cross Site Scripting	The attacker can steal a legitimate web application user's session, rather than modify the behavior of the application itself.	User input which contains special char sets is not correctly sanitized, thus written in clear text into the application's pages.

Mistakes when writing code

Vulnerability	Impact	Description
V-006 Missing HTTP Only cookie protection	In a XSS scenario, the attacker can get access to the session cookie.	The cookie does not have the flag HTTP Only, which avoids access to the cookie via Javascript.
V-007 Missing Secure cookie protection	In a Man in the Middle and protocol downgrade attack scenario, the session cookie can be intercepted in clear text by the attacker.	The Secure flag of the cookie, which prevents it from passing through not encrypted channels, is not enabled.
V-008 Unsafe sensitive page Caching	An attacker can get access to private web pages, which are saved in the victim's browser cache, rather than in a Proxy through which the requests have passed by.	Headers telling to the browser and the proxy to not save passwords in the cache, are not specified.
V-009 Autocomplete not disabled on password field	Passwords from the "password" fields in the application can be saved in clear text on the victim's machines, thus allowing attackers or malwares to obtain them very easily.	Wherever the attribute "autocomplete" is not present, rather that it's not set as "off", passwords can be saved by the browser in clear text, allowing autocomplete.
V-010 Missing X-Content-Type-Options header protection	While adding malicious code inside not-malicious files, some browsers could execute it automatically, processing the file in a different manner from the expected one.	Not setting the header "Missing X-Content-Type-Options" to "nosniff", some browsers could process malicious code without checking the real file format.
V-011 Missing X-Frame-Options header protection	The page can be used by an attacker in order to launch clickjacking type attacks.	Without the right headers, the page can be inserted into IFRAMEs in domains which are different from the legal, authorized one.

Mistakes when writing code

Vulnerability	Impact	Description
V-012 OPTIONS method enabled	An attacker can learn all of the http methods available in order to plan an attack.	The Web Server command OPTIONS returns all of the HTTP commands which can be used.
V-013 TRACE method enabled	An attacker may use this method on different attack types, such as bypassing the HTTP Only flag, rather than as a support of different Renegotiation vulnerabilities.	The debug method TRACE allows to return arbitrary text from the Web Server to the client.
V-014 Cross-User Interaction	A platform's user can get access and modify those data belonging to different users. The same issues applies as well among profiles of different user's type.	In some cases, the data visualization and modification pages, related to different types of users, do not verify correctly if the user which is changing them is the owner as well.
V-015 SSL/TLS Renegotiation	Whenever a Man in the Middle attack happens, the attacker can renegotiate the protocol, thus obtaining data which can be decrypted. In some cases, it's possible also to intercept in clear text the communication.	Protocol's renegotiation allows switching the communication from a secure protocol to a weaker one; it is also possible to run Reflection type attacks.
V-016 Weak SSL/TLS Ciphers	An attacker which has obtained the traffic dump, can easily decrypt it through widely deployed and available techniques.	During the secure SSL/TLS connection, it can be selected ciphers easy to decrypt.
V-017 Slow Loris DOS vulnerability	A malicious user can overload the Web Server with requests, thus limiting its own availability.	The Web Server accepts very long connections and not-existent headers, allowing a malicious user to allocate plenty of resources to the server, for extremely long timings.

Mistakes when writing code

Vulnerability	Impact	Description
V-018 HTTP Session not expire	A malicious user can overload the Web Server with requests, thus limiting its own availability.	The Web Server accepts very long connections and not-existent headers, allowing a malicious user to allocate plenty of resources to the server, for extremely long timings.
V-019 Cross Site Request Forgery	An attacker is able to open a link to the victim, through a validated session, thus executing unexpected, unwanted operations in the application itself.	The application does not implement in its forms any anti-CSRF tokens, so that the Web Server cannot verify if the requests are legitimate ones, rather than pushed by an attacker.
V-020 Potential denial of service using Mail service	A malicious user can send out huge amounts of emails to an arbitrary recipient, through the server which is hosting the application.	There's no check of the amount of emails sent from the automated-sending systems which check for the account confirmation.
V-021 Change domain on change password mail	An attacker can insert links which are different from those of the organization web site into the confirmation emails, which are addressed to the victim, thus allowing phishing attacks.	The application allows the arbitrary choice of the domain which generates the confirmation link for the email matched to an account.
V-022 Improper error handling	The application shows in clear text the errors' stacktrace, allowing the attacker to understand how it works.	Errors' stacktraces are active if some parameters are missing rather than anomalies.

Mistakes when writing code

Vulnerability	Impact	Description
V-023 User disclosure	It's possible to run a bruteforce attack on the application's internal IDs (i.e.: employee or student's personal identification number), in order to discover those existing ones through the login page.	Error messages such as "User does not exist" and "Password incorrect" can be displayed in a different return message from a not-authenticated user.
V-024 Improper CAPTCHA implementation	The registration CAPTCHA is not deployed correctly, allowing a remote attacker to overload the user's DB, bypassing the anti-automation controls.	CAPTCHA is easy to bypass, since it is not deployed correctly.
V-025 Concurrent Session Access	Whenever an attacker is connected with the same account of the victim, the authorized user can't realize, and two concurrent sessions do exist.	For some application roles, there is no check if any concurrent sessions for authenticated users do exist.
V-026 Information disclosure	An attacker can learn useful information related to the Web Server software and its version/release.	The Web Server returns in its answers all of the information related to the name and version of the software.

Conclusions

This presentation focused on **different mistakes which are made by organizations** from all over the world, **no matter their size and maturity into Information Security**.

While **different approaches and the use of different solutions clearly depends on available resources** (budgets, amount of IT staff, seniority and skills of system administrators and programmers), we think that **everything should start from tasks which are very easy to deploy inside all of the organizations**: internal awareness, and training towards your employees and colleagues.

It is **a process which helps out IT and InfoSec people raising the understanding of their everyday activities towards the management**, and those **colleagues from different departments**, in order to pursue altogether a shared goal: **the information security of your Organization**.

Last but not least, we have seen **how much the lack of secure programming**, and **Secure SLDC**, may **dramatically impact on the overall security** of our organizations, **providing the right "back entrance"** for attackers, **and enemies**.

References

- "World's biggest data breach": http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/
- Australian Signals Directorate "Strategies to Mitigate Targeted Cyber Intrusions": http://www.asd.gov.au/infosec/top-mitigations/mitigations-2014-table.htm
- Open-source based Cyber Intelligence portal: https://brica.de/
- Slow loris DoS: http://it.wikipedia.org/wiki/Slowloris

Contacts, Q&A

- **Need** anything, got **doubts**, wanna **ask me smth**?
  - rc [at] security-brokers [dot] com
  - Pub key: http://www.security-brokers.com/keys/rc_pub.asc

Thanks for your attention!

QUESTIONS?