RSA CONFERENCE 2014
ASIA PACIFIC & JAPAN

EAS-SEC Project: Securing Enterprise Business Applications

SESSION ID: SEC-W06

Alexander Polyakov

CTO
ERPScan
@Twitter sh2kerr

ERPScan
Security Monitoring Suite for SAP

Alexander Polyakov

- CTO of the ERPScan inc
- EAS-SEC.org President
- Business application security expert
- R&D Professional of the year by Network Product Guide

a.polyakov@erpscan.com

Twitter: @sh2kerr

ERPScan
Security Monitoring Suite for SAP

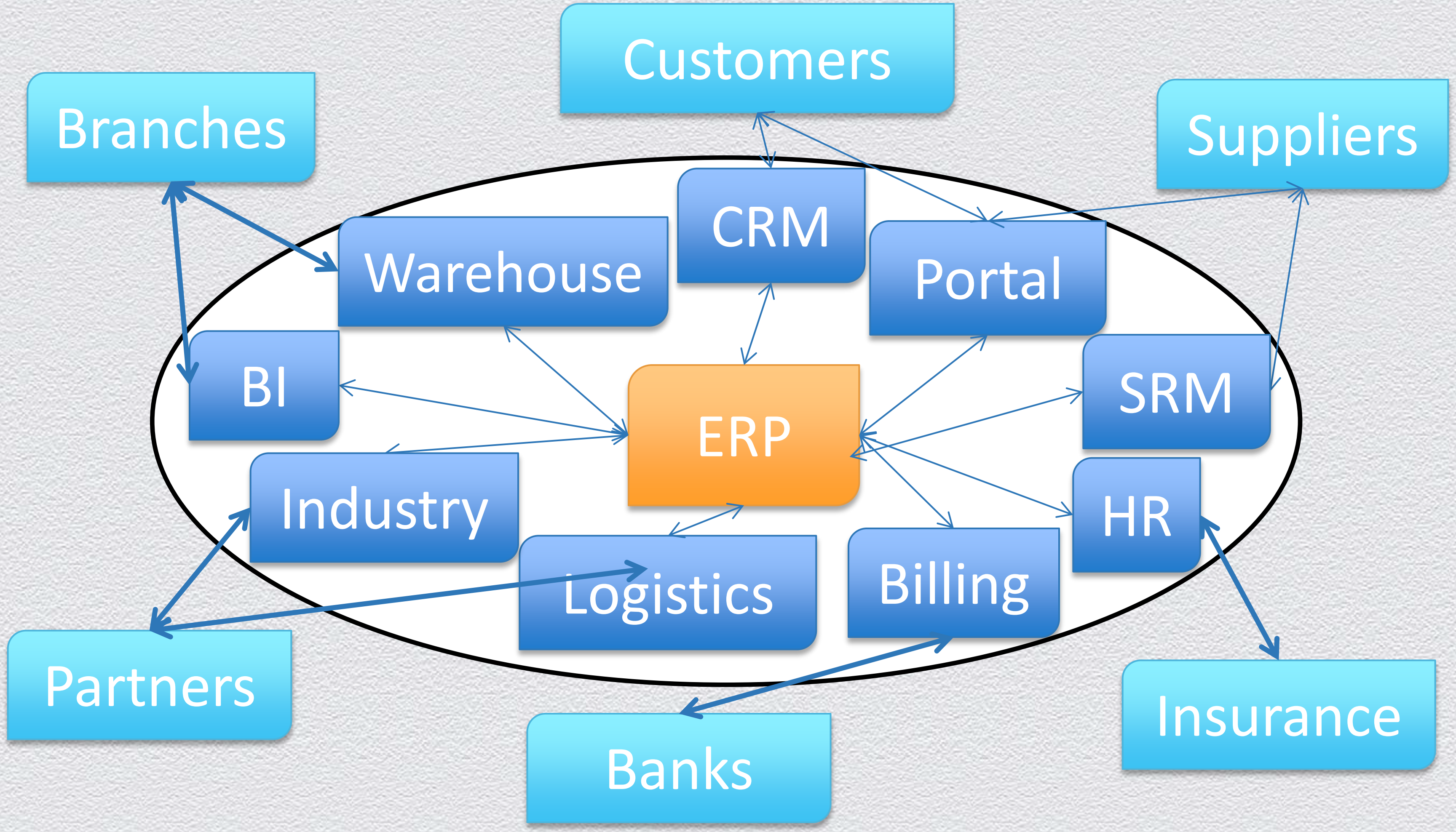
Intro

- Intro
- Big companies and critical systems
- Problems
- How easy it is to break
- Current security approaches
- EAS-SEC
- EAS-SEC for SAP
- Results taken from latest awareness publications
- Conclusion

Big companies

- Oil and Gas
- Manufacturing
- Logistics
- Financials
- Nuclear
- Retail
- Telecommunication
- etc

Big companies inside



ERPScan — invest in security to secure investments

If business applications are popular?

SAP

- More than 246000 customers worldwide
- 86% of Forbes 500

Oracle

- 100% of Fortune 100

Microsoft

- More than 300,000 businesses worldwide choose Microsoft Dynamics ERP and CRM software

What can happen

- Espionage
  - Stealing financial information
  - Stealing corporate secrets
  - Stealing supplier and customer lists
  - Stealing HR data
- Sabotage
  - Denial of service
  - Modification of financial reports
  - Access to technology network (SCADA) by trust relations
- Fraud
  - False transactions
  - Modification of master data

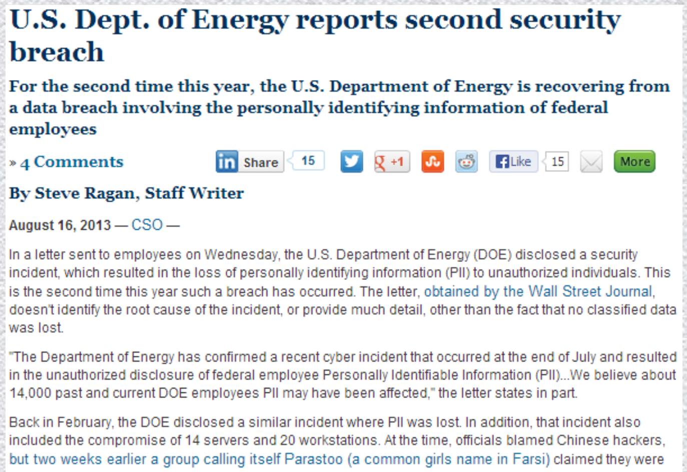
Industrial espionage

- Autocad virus
- Stealing critical documents
- Send them potentially to china

http://www.telegraph.co.uk/technology/news/9346734/Espionage-virus-sent-blueprints-to-China.html

Sabotage

- Victim: US Department of Energy
- Target: HR system
- Result: unauthorized disclosure of federal employee Personally Identifiable Information
- Real example of stealing 14000 of records



U.S. Dept. of Energy reports second security breach

For the second time this year, the U.S. Department of Energy is recovering from a data breach involving the personally identifying information of federal employees

By Steve Ragan, Staff Writer

August 16, 2013 — CSO —

In a letter sent to employees on Wednesday, the U.S. Department of Energy (DOE) disclosed a security incident, which resulted in the loss of personally identifying information (PII) to unauthorized individuals. This is the second time this year such a breach has occurred. The letter, obtained by the Wall Street Journal, doesn't identify the root cause of the incident, or provide much detail, other than the fact that no classified data was lost.

"The Department of Energy has confirmed a recent cyber incident that occurred at the end of July and resulted in the unauthorized disclosure of federal employee Personally Identifiable Information (PII)...We believe about 14,000 past and current DOE employees PII may have been affected," the letter states in part.

Back in February, the DOE disclosed a similar incident where PII was lost. In addition, that incident also included the compromise of 14 servers and 20 workstations. At the time, officials blamed Chinese hackers, but two weeks earlier a group calling itself Parastoo (a common girls name in Farsi) claimed they were

Fraud

- The Association of Certified Fraud Examiners (**ACFE**) survey showed that U.S. organizations lose an estimated **7**% of annual revenues to fraud.
- Average loss per organization for fraud $500k + collateral damage
- PWC Survey: 3000 org in 54 countries – 30%were victims of economic crime in prev 12 month
- Real examples that we met:
  - Salary modification
  - Material management fraud
  - Mistaken transactions (big items like Pump Jack)

What can be next?

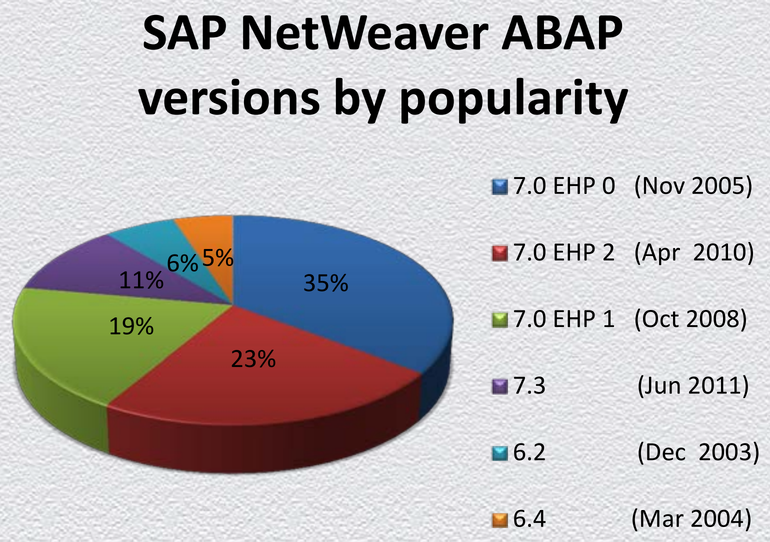
Just imagine what could be done by breaking:

- One ERP system
- All Business applications of a company
- All ERP Systems of one particular country

How easy it is to break them?

Ease of attack preparation

- Price of vulnerability is low
- Patching is nightmare
- Payload development is easy
- Interconnection is high
- Availability via internet



Systems are highly connected

- Systems are highly connected with each other by trust relationship
- Even between companies they are connected by ESB systems
- Remember also SSRF?

  http://cwe.mitre.org/data/definitions/918.html
- Second place in Top 10 web application techniques 2012
- Allows to bypass firewall restrictions and directly connect to protected systems via connected systems

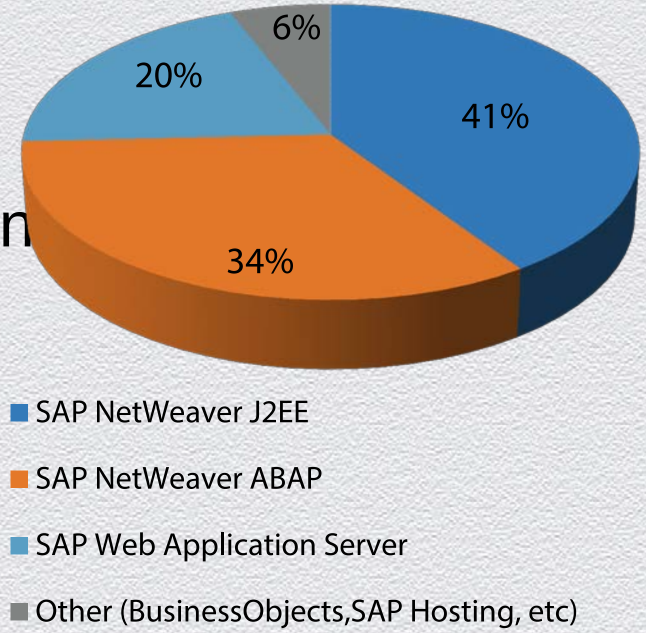
Business applications on the Internet

- Companies have Portals, SRMs, CRMs remotely accessible
- Companies connect different offices by ESB
- SAP users are connected to SAP via SAPRouter
- Administrators open management interfaces to the Internet for remote control

Business applications on the Internet

SAP HTTP Services can be easily found on the Internet:

- inurl:/irj/portal
- inurl:/IciEventService sap
- inurl:/IciEventService/IciEventCon
- inurl:/wsnavigator/jsps/test.jsp
- inurl:/irj/go/km/docs/



A total of 3741 server with different SAP web applications were found

ERPScan — invest in security to secure investments

SAP Router

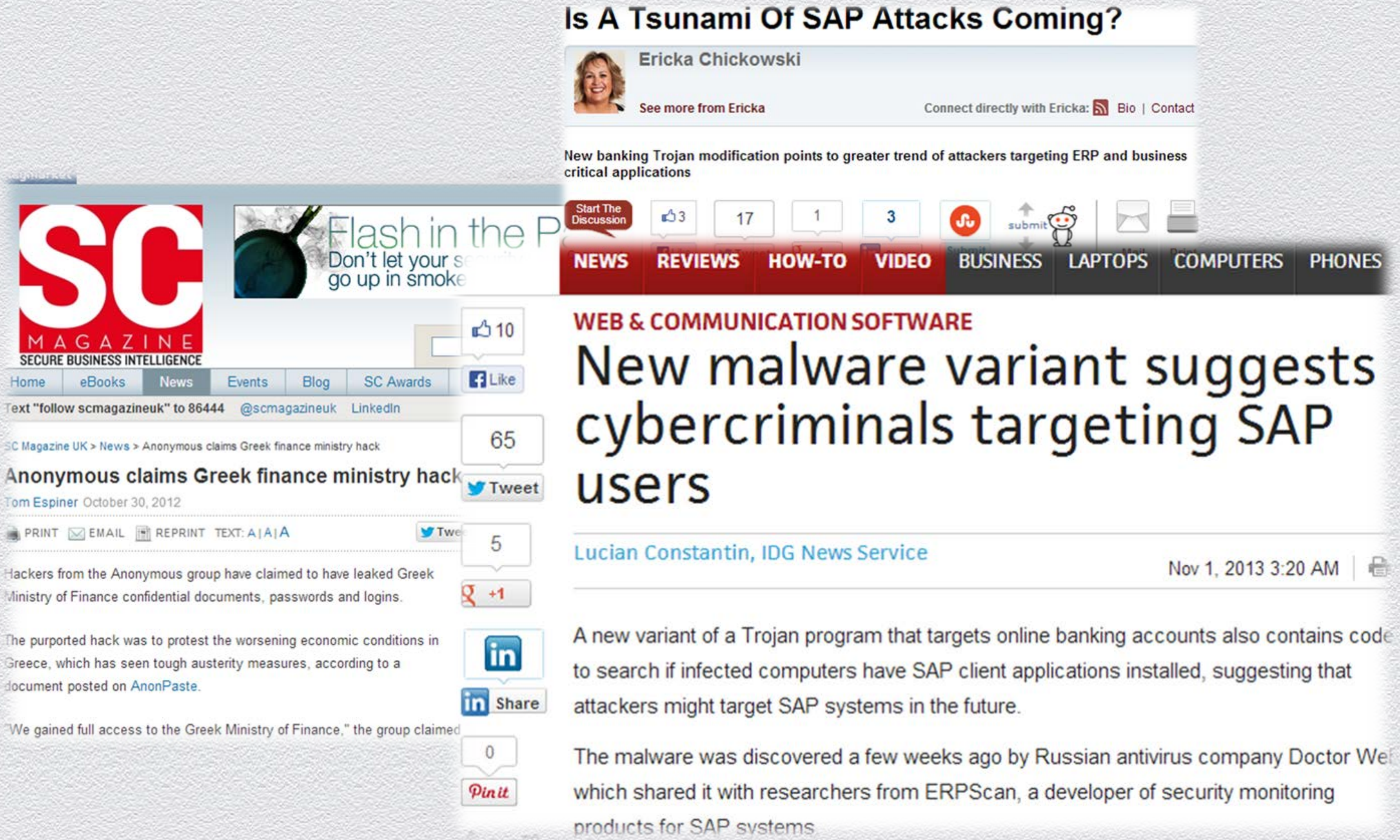
- Special application proxy
- Transfers requests from Internet to SAP (and not only)
- Can work through VPN or SNC
- Almost every company uses it for connecting to SAP to download updates
- Usually listens to port 3299
- Internet accessible (Approximately 5000 IP’s)
- http://www.easymarketplace.de/saprouter.php

SAP Router vulnerability

- Remote Code Execution vulnerability
- CVSS 9.3
- Nominated for top 5 server-side vulnerabilities 2013

ERPScan — invest in security to secure investments

SAP Malware



Is A Tsunami Of SAP Attacks Coming?

Ericka Chickowski

See more from Ericka

Connect directly with Ericka: Bio | Contact

New banking Trojan modification points to greater trend of attackers targeting ERP and business critical applications

SC MAGAZINE SECURE BUSINESS INTELLIGENCE

Text "follow scmagazineuk" to 86444 @scmagazineuk LinkedIn

SC Magazine UK > News > Anonymous claims Greek finance ministry hack

Anonymous claims Greek finance ministry hack

Tom Espiner October 30, 2012

Hackers from the Anonymous group have claimed to have leaked Greek Ministry of Finance confidential documents, passwords and logins.

The purported hack was to protest the worsening economic conditions in Greece, which has seen tough austerity measures, according to a document posted on AnonPaste.

"We gained full access to the Greek Ministry of Finance," the group claimed

WEB & COMMUNICATION SOFTWARE

New malware variant suggests cybercriminals targeting SAP users

Lucian Constantin, IDG News Service

Nov 1, 2013 3:20 AM

A new variant of a Trojan program that targets online banking accounts also contains code to search if infected computers have SAP client applications installed, suggesting that attackers might target SAP systems in the future.

The malware was discovered a few weeks ago by Russian antivirus company Doctor Web which shared it with researchers from ERPScan, a developer of security monitoring products for SAP systems.

ERPScan — invest in security to secure investments

SAP Security

Why we do need a new guide?

3 areas of Business Application Security

Business logic security (SOD)
Prevents attacks or mistakes made by insiders

Custom Code security
Prevents attacks or mistakes made by developers

Application platform security
Prevents unauthorized access both insiders and remote attackers

- For WEB we have OWASP, WASC
- For Network and OS we have NIST,SANS
- But what about Enterprise Business Applications?

Why? (1)

- Questions like "why?" and "what for" are the alpha the omega of every research
- We were asked more often than any other was: *“Guys, you are awesome! And you are doing a great job so far, finding so many problems in our installations. It's absolutely fantastic, but we don’t know, where should we start to solve them. Could you provide us with top 10/20/50/100/ [put your favorite number here] most critical bugs in every area?”*

Why? (2)

- We had to do something completely different from just top-10 of the most critical bugs
- Even if you patch all vulnerabilities there still could remain lots of problems: Access control, configuration, logs
- The number one challenge is to understand all security areas of EAS and to have an opportunity for every area select a number of most critical issues.

Why? (3)

- We started to analyze existing guidelines and standards.
  - High level policies: NIST,SOX,ISO,PCI-DSS
  - Technical guides: OWASP, WASC, SANS 25, CWE
  - SAP Guides:
    - Configuration of SAP NetWeaver® Application Server Using ABAP by SAP
    - ISACA Assurance (ITAF) by ISACA
    - DSAG by German SAP User Group.
- All those standards are great, but unfortunately, all of them have at least one big disadvantage.

SAP Security Guidelines

- Guidelines made by SAP
- First official SAP guide for technical security of ABAP stack
- Secure Configuration of SAP NetWeaver® Application Server Using ABAP
- First version - 2010 year, version 1.2 – 2012 year
- For rapid assessment of most common technical misconfigurations in platform
- Consists of 9 areas and 82 checks
- Ideas as a second step and give more details to some of EAS-SEC standard areas

  http://www.sdn.sap.com/irj/scn/go/portal/prtroot/docs/library/uuid/f0d2445f-509d-2d10-6fa7-9d3608950fee?overridelayout=true

SAP Security Guidelines

- **Advantages:** very brief, but quite informative (only 9 pages) and covers application platform issues, applicable for every ABAP- based platform either ERP or Solution manger or HR, it doesn't matter.
- **Disadvantages:** 82 checks is still a lot for a first brief look on secure configuration. But what's more important, standard doesn't cover access control issues and logging and even in platform security miss some things. Finally, it gives people false sense of security, if they cover all checks. But it wouldn't be completely true.

ISACA Assurance (ITAFF)

- Guidelines made by ISACA
- Checks cover configuration and access control areas
- First most full compliance
- There were 3 versions published in 2002, 2006, 2009 (some areas are outdated nowadays)
- Technical part covered less than full info about access control and miss some of the critical areas
- The biggest advantage is a big database of access control checks
- Consists of 4 parts and more than 160 checks
- Ideal as a third-step-guide and very useful for it’s detailed coverage of access control

ISACA Assurance (ITAFF)

- **Advantages:** detailed coverage of access control checks.
- **Disadvantages:** Outdated. Technical part is missing. Guideline consists of too many checks, and can't be easily applicable by non-SAP specialist. Also it can't be applicable to any system without prior understanding of the business processes. And finally, this guideline could be found officially only as part of the book or you should be at least an ISACA member to get it.

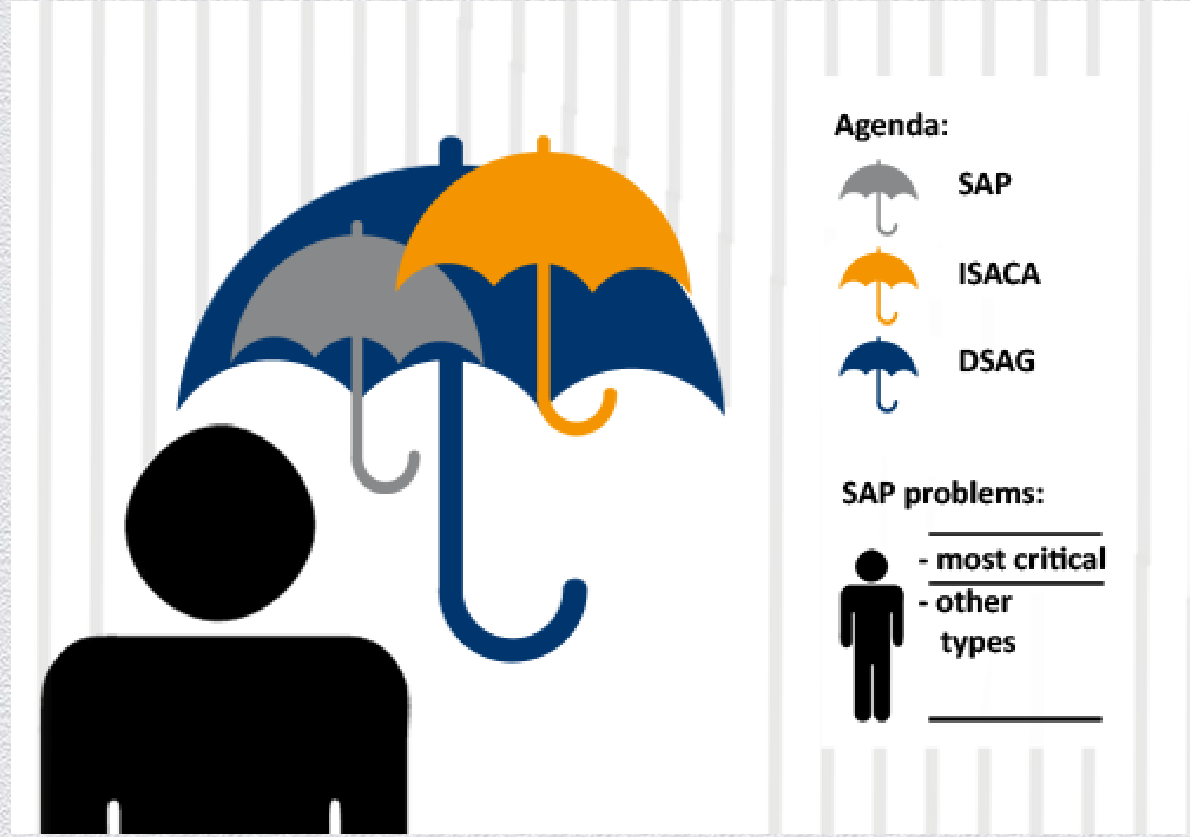
DSAG

- Set of recommendations from Deutsche SAP Uses Group
- Checks cover all security areas from technical configuration and source code to access control and management procedures
- Currently biggest guideline about SAP Security
- Last version in Jan 2011
- Consists of 8 areas and 200+ checks
- Ideal as a final step for securing SAP but consists of many checks which needs additional decision making which is highly depends on installation. *http://www.dsag.de/fileadmin/media/Leitfaeden/110818_Leitfaden_Datenschutz_Englisch_final.pdf*

DSAG

- **Advantages:** Ideal as a final step for securing SAP. Great for SAP Security administrators, covers almost all possible areas.
- **Disadvantages:** Unfortunately, has the same problem as ISACA. It is too big for a starter, and no help at all for Security people who are not familiar with SAP. Also it can't be directly applicable to every system without prior understanding of business processes. Many checks are recommendations and user should think by himself, if they are applicable in each every case.

Compliance


Agenda:
SAP
ISACA
DSAG
SAP problems:
- most critical
- other types

EAS-SEC

- The authors' efforts were to make this list as brief as possible
- to cover the most critical threats for each area.
- be easily used not only by SAP/ERP security experts but by every Security specialist
- should also provide comprehensive coverage of all critical areas of SAP Security.
- At the same time, developing of the most complete guide would be a never-ending story
- So, we talking about 80/20 rules, and we will implement it in SAP Security

EAS-SEC

- Developed by ERPScan:
- First release 2010
- Second edition 2013
- 3 main areas
  - Implementation Assessment
  - Code review
  - Awareness

Rapid assessment of Business Application security

EASSEC Implementation Assessment

EASSSEC-AIVA	Access	Criticality	Easy to exploit	% of vulnerable systems
1. Lack of patch management	Anonymous	High	High	99%
2. Default Passwords for application access	Anonymous	High	High	95%
3. Unnecessary enabled functionality	Anonymous	High	High	90%
4. Open remote management interfaces	Anonymous	High	Medium	90%
5. Insecure configuration	Anonymous	Medium	Medium	90%
6. Unencrypted communication	Anonymous	Medium	Medium	80%
7. Access control and SOD	User	High	Medium	99%
8. Insecure trust relations	User	High	Medium	80%
9. Logging and Monitoring	Administrator	High	Medium	98%

Custom code assessment

- ABAP, Peoplecode, X++ – as any other language can have a vulnerabilities
- Also it can be used for writing backdoors
- Development inside a company is almost without any control
- Developer access to system == god mode ON
- Current approaches like WASC,OWASP mainly for WEB

Source code review

- EASAD-9
- Full name:
    - Enterprise Application Systems Application Development
- Describes 9 areas or source code issues for business languages
- Universal categories for different languages and systems (SAP,Oracle,Dynamix,Infor…..)
- Categorized based on criticality and probability of exploitation

EASSEC Implementation Assessment

EASSSEC-AIVA	Access	Criticality	Easy to exploit	% of vulnerable systems
Code injections	Anonymous	High	High	99%
Critical calls	Anonymous	High	High	95%
Missing authorization checks	Anonymous	High	High	90%
1. 4Path traversal	Anonymous	High	Medium	90%
1. 5. Modification of displayed content	Anonymous	Medium	Medium	90%
1. 6. Backdoors	Anonymous	Medium	Medium	80%
7. Access control and SOD	User	High	Medium	99%
8. Insecure trust relations	User	High	Medium	80%
9. Logging and Monitoring	Administrator	High	Medium	98%

EASAD - 9 categories

1. Code injections
2. Critical calls
3. Missing authorization checks
4. Path traversal
5. Modification of displayed content
6. Backdoors
7. Covert channels
8. Information disclosure
9. Obsolete statements

SAP Security

EAS-SEC for SAP

EAS-SEC for NetWeaver (EASSEC-AIVA-ABAP)

Enterprise Application Systems Vulnerability Assessment – for NetWeaver ABAP

- First standard of series EAS-SEC
- Rapid assessment of SAP security in 9 areas
- Contains 33 most critical checks
- deal as a first step
- Also contain information for next steps
- Categorized by priority and criticality

Lack of patch management

- [EASAI-NA-01] Component updates
- [EASAI-NA-02] Kernel updated

What next: *Other components should be be updated separately – SAP Router, SAP Gui, SAP NetWEaver J2EE, SAP BusinessObjects. And also OS and Database.*

Default passwords

- [EASAI-NA-03] Default password check for user SAP*
- [EASAI-NA-04] Default password check for user DDIC
- [EASAI-NA-05] Default password check for user SAPCPIC
- [EASAI-NA-06] Default password check for user MSADM
- [EASAI-NA-07] Default password check for user EARLYWATCH

What next: *Couple of additional SAP components also use their own default passwords. For example services SAP SDM and SAP ITS in their old versions has default passwords. After you check all default passwords you can start with bruteforcing for simple passwords.*

Unnecessary enabled functionality

- [EASAI-NA-08] Access to RFC-functions using SOAP interface
- [EASAI-NA-09] Access to RFC-functions using FORM interface
- [EASAI-NA-10] Access to XI service using SOAP interface

What next: *You should analyze about 1500 other services which are remotely enabled if they are really needed and also disable unused transactions, programs and reports.*

Open remote management interfaces

- [EASAI-NA-11] Unauthorized access to SAPControl service
- [EASAI-NA-12] Unauthorized access to SAPHostControl service
- [EASAI-NA-13] Unauthorized access to Message Server service
- [EASAI-NA-14] Unauthorized access to Oracle database

What next: *Full list of SAP services you can get from document [TCP/IP Ports Used by SAP Applications.](#) Also you should take care about 3*rd *party services which can be enabled on this server.*

Insecure configuration

- [EASAI-NA-15] Minimum password length
- [EASAI-NA-16] User locking policy
- [EASAI-NA-17] Password compliance to current standards
- [EASAI-NA-18] Access control to RFC (reginfo.dat)
- [EASAI-NA-19] Access control to RFC (secinfo.dat)

What next: *First of all you can look at (Secure Configuration of SAP NetWeaver® Application Server Using ABAP) document for detailed configuration checks. Afterwards you can pass throught detailed documents for each and every SAP service and module*

http://help.sap.com/saphelp_nw70/helpdata/en/8c/2ec59131d7f84ea514a67d628925a9/frameset.htm

Access control and SOD conflicts

- [EASAI-NA-20] Users with SAP_ALL profile
- [EASAI-NA-21] Users which can run any program
- [EASAI-NA-22] Users which can modify critical table USR02
- [EASAI-NA-23] Users which can execute any OS command
- [EASAI-NA-24] Disabled authorization checks

What next: *There are at leas about 100 critical transactions only in BASIS and approximately the same number in each other module. Detailed information can be found in ISACA guidelines . After that you can start with Segregation of Duties.*

Unencrypted connections

- [EASAI-NA-25] Use of SSL for securing HTTP connections
- [EASAI-NA-26] Use of SNC for securing SAP Gui connections
- [EASAI-NA-27] Use of SNC for securing RFC connections

What next: *Even if you use encryption you should check how is it configured for every type of encryption and for every service because there are different complex configurations for each of encryption type. For example latest attacks on SSL like BEAST and CRIME require companies to use more complex SSL configuration.*

Insecure trusted connections

- [EASAI-NA-28] RFC connections with stored authentication data
- [EASAI-NA-29] Trusted systems with lower security

What next: *Check other ways to get access to trusted systems such as database links o use of the same OS user or just use of the same passwords for different systems.*

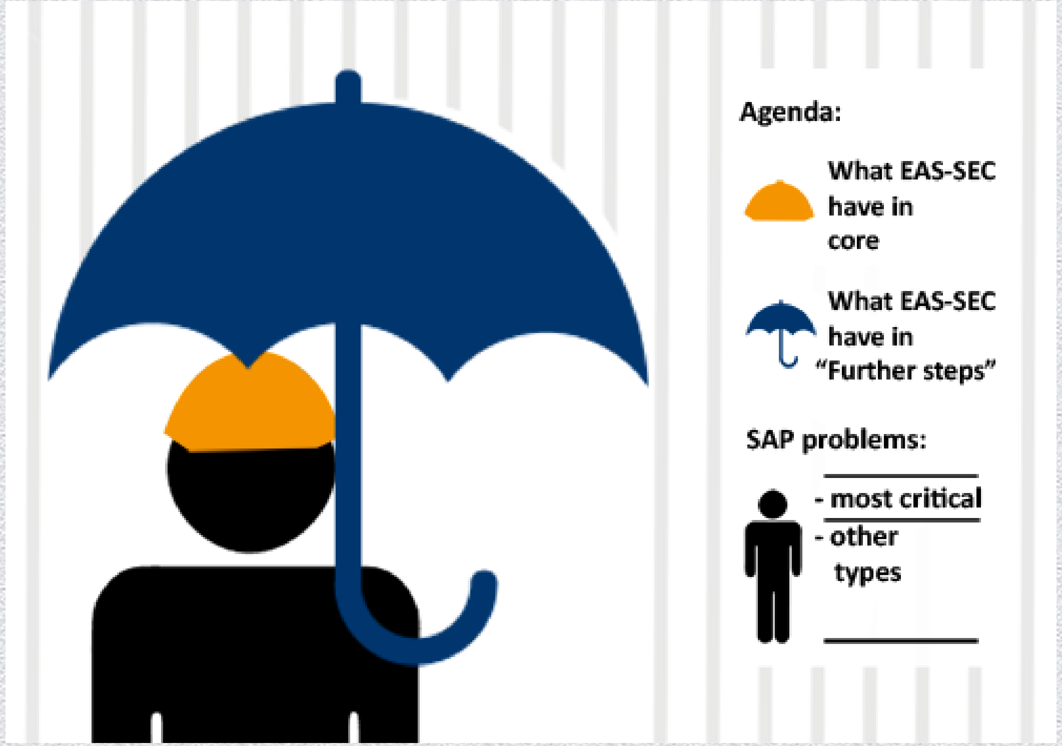
Logging and Monitoring

- [EASAI-NA-30] Logging of security events
- [EASAI-NA-31] Logging of HTTP requests
- [EASAI-NA-32] Logging of table changes
- [EASAI-NA-33] Logging of access to Gateway

What next: *There are about 30 different types of log files in SAP. The next step after properly enabling main of them you should properly configure complex options such as what exact tables to monitor for changes, what kind of events to analyze in security events log, what types of Gateway attacks should be collected and so on. Next step is to enable their centralized collection and storage and then add other log events.*

Results

- For successful project it is not enough to make guidelines. It is necessary to do some research and reviews. Awareness is also very helpful in security


Agenda:
What EAS-SEC have in core
What EAS-SEC have in "Further steps"
SAP problems:
- most critical
- other types

ERPScan — invest in security to secure investments

Awareness

- SAP Security in figures 2011
- SAP Security in figures 2013
- 3000 vulnerabilities in SAP
- SAP Security in figures 2014 (coming soon)

3000 vulnerabilities in SAP

According to official information from SAP portal, more than 3000 vulnerabilities have been closed by SAP

- **“Interest in SAP security is growing exponentially”** - number of vulnerabilities found by 3rd parties comparing to vulnerabilities patched by SAP has grown from about 10% in late 2000s to 60-70% in recent monthly updates.

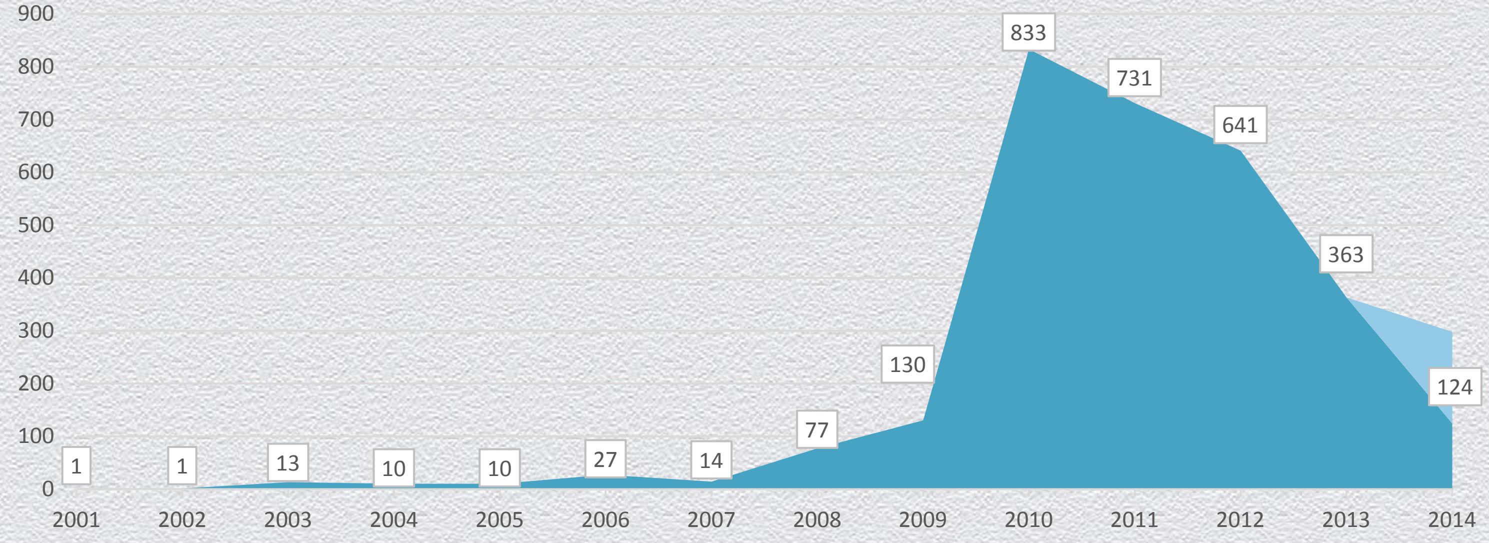
Awareness

"Percentage of vulnerabilities in SAP is much higher that people usually think" - number of vulnerabilities closed by SAP equals to about 5% of all vulnerabilities ever published on the Internet. (60000+ vs 3000+)

Place	Vendor	Number of vulnerabilities
1	Microsoft	2934
2	Apple	1927
3	Oracle	1531
4	IBM	1457
5	SUN	1384
6	CISCO	1147
7	Mozilla	1195
8	Linux	944
9	HP	925
10	Adobe	818

Awareness

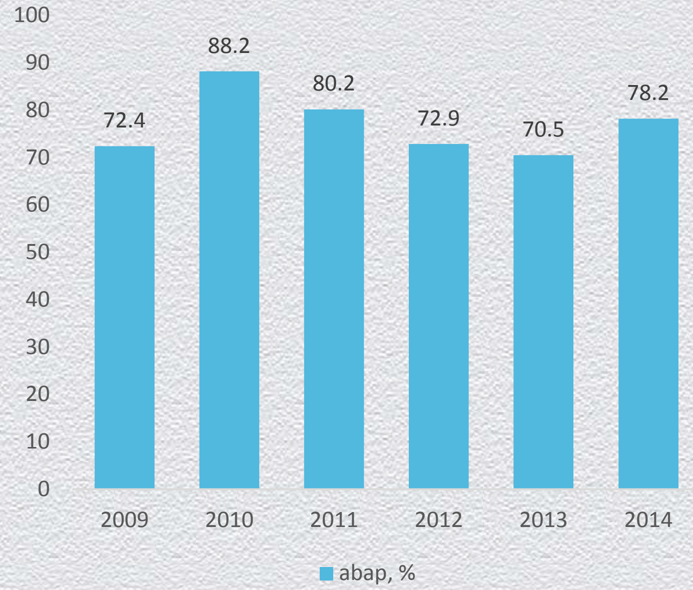
"SAP is making good steps in SDLC" - number of vulnerabilities in SAP per month has decreased approximately 2 times comparing to the high peak in 2010.

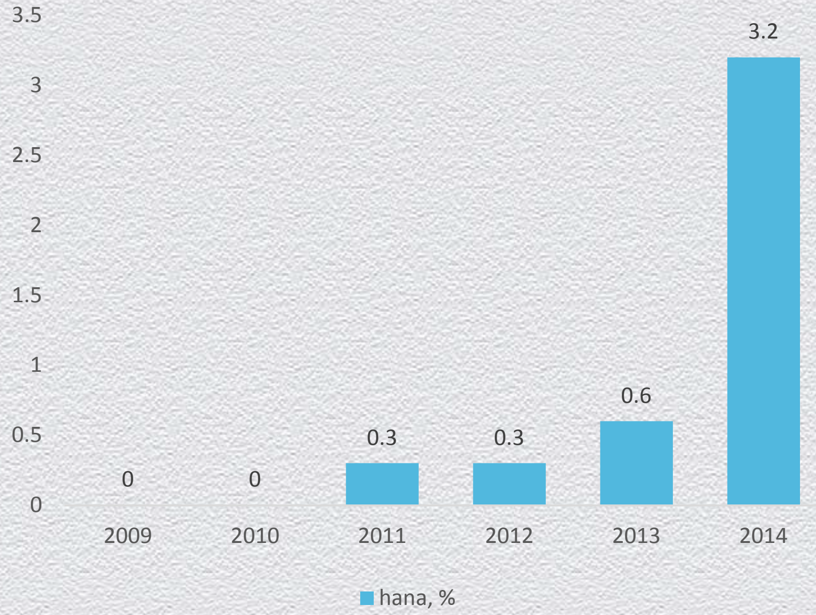


ERPScan — invest in security to secure investments

Awareness

"Interest in hacking of NEW SAP products is growing" - number of issues found in new SAP products, like SAP HANA, is growing faster than in others, although there are about 10 issues in total.

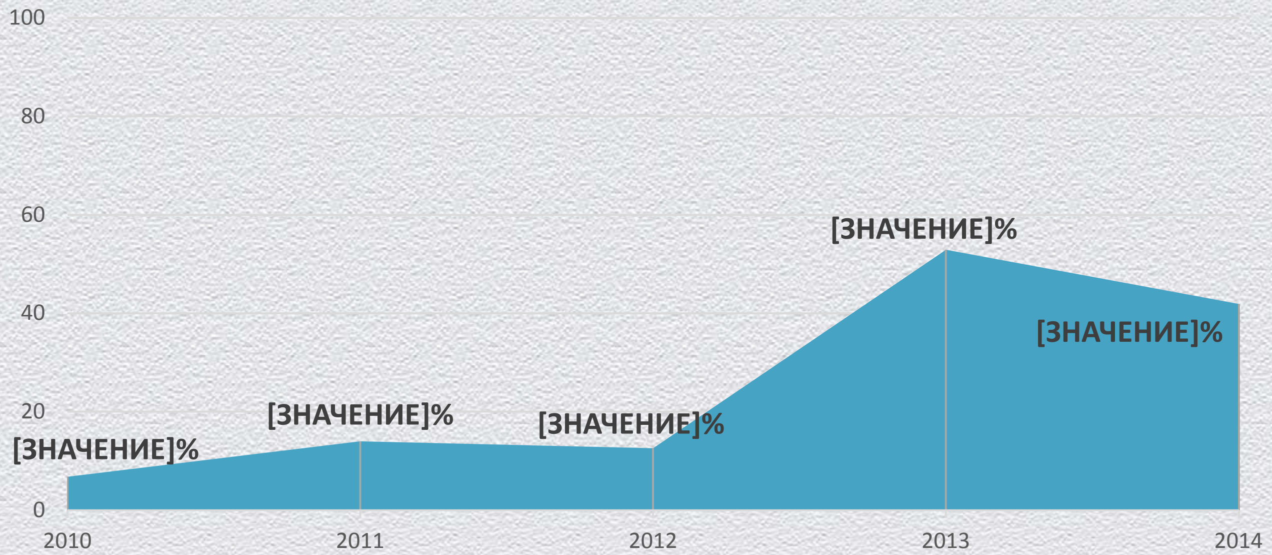




ERPScan — invest in security to secure investments

Awareness

“Interest in SAP security is growing exponentially” - number of vulnerabilities found by 3rd parties comparing to vulnerabilities patched by SAP has grown from about 10% in late 2000s to 60-70% in recent monthly updates.

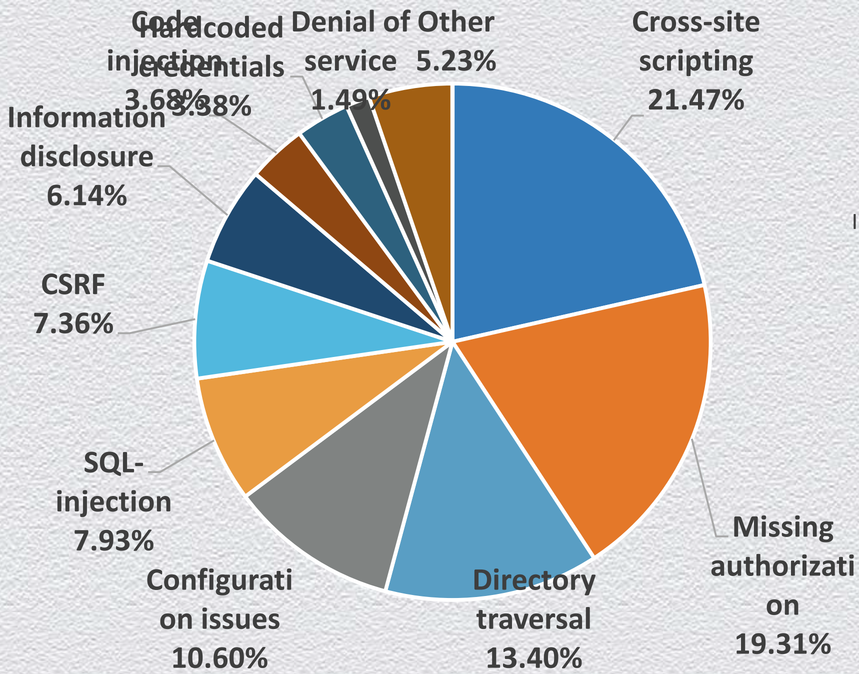


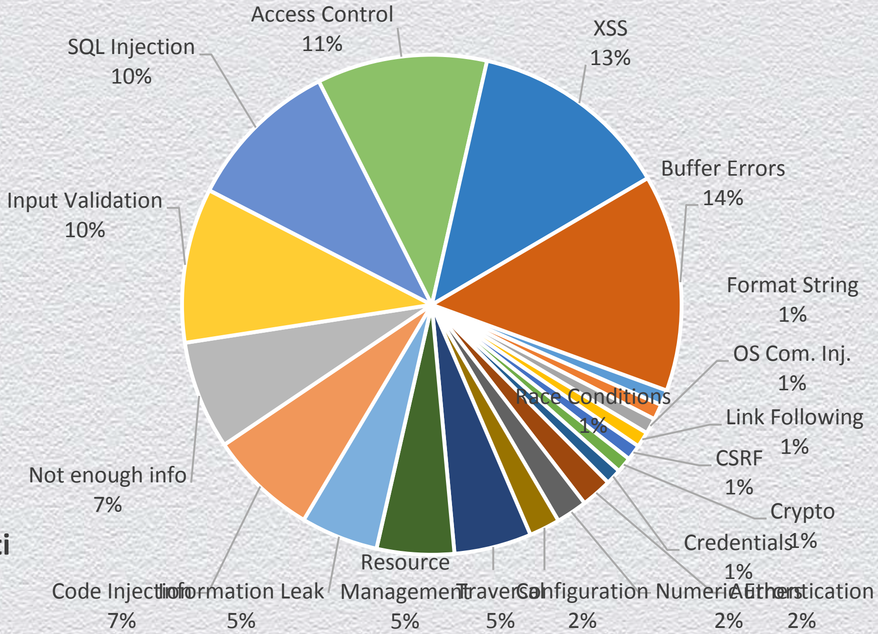
ERPScan — invest in security to secure investments

ERPScan
Security Monitoring Suite for SAP

Awareness

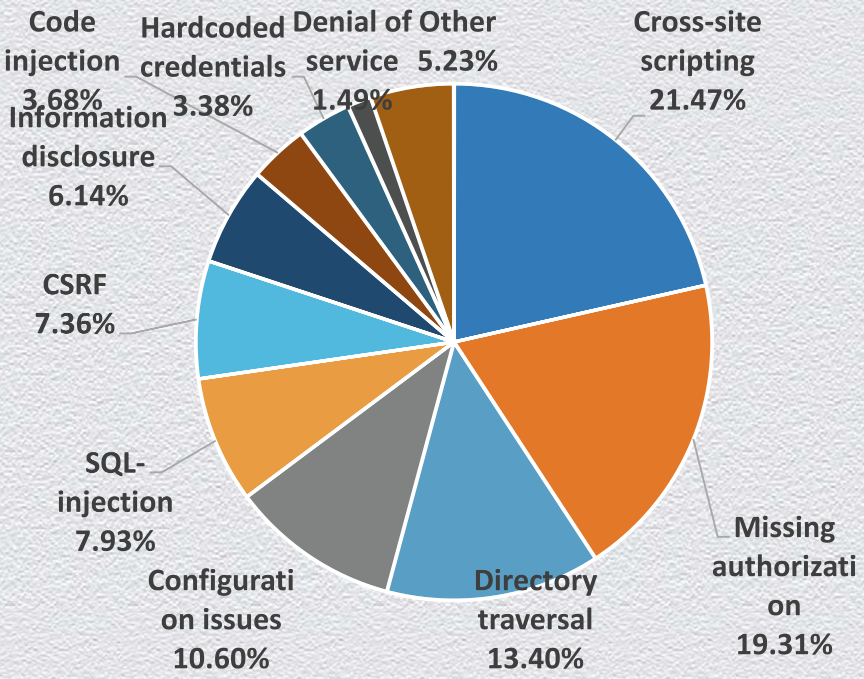
“What is popular with traditional security is not always popular with SAP security” - memory corruption vulnerabilities are 7 times less popular in SAP than in general types of products.

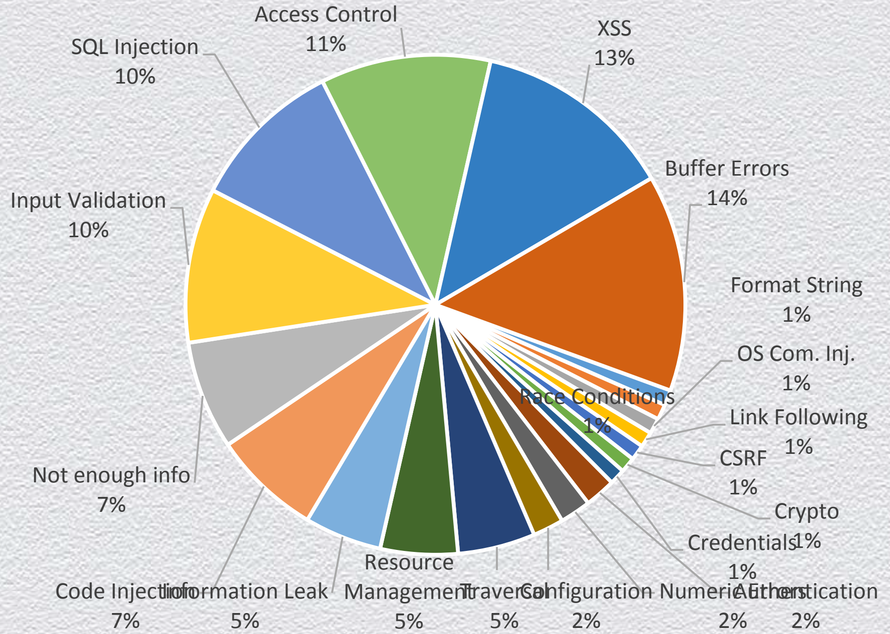




Awareness

“SAP is a very complicated system, and a significant part of security measures lies on the shoulders of the administrators” - configuration issues in SAP are 5 times more popular than in general types of products.





Next Steps

- Release similar compliance guidelines for other applications and languages
- Update eas-sec.org
- Spread this initiative

Download security guidelines:

http://erpscan.com/wp-content/uploads/2014/04/EASSEC-PVAG-ABAP-THE-SAP-NETWEAVER-ABAP-PLATFORM-VULNERABILITY-ASSESSMENT-GUIDE-2014-3.11.53-AM.pdf

Download awareness publications:

http://erpscan.com/wp-content/uploads/2014/02/SAP-Security-in-Figures-A-Global-Survey-2013.pdf

http://erpscan.com/wp-content/uploads/2012/06/SAP-Security-in-figures-a-global-survey-2007-2011-final.pdf

Ask

Please

?

Your Questions

RSA CONFERENCE 2014
ASIA PACIFIC & JAPAN

Thank You for Your Attention!

ERPScan
Security Monitoring Suite for SAP