ERP-SEC
HARMONIZING BUSINESS AND SECURITY

BSIDES LUXEMBOURG


# Smart SAP CyberSecurity

Automating SAP Security patches – A customer case

# ERP Security

- Experts in SAP Security assessments and hardening
- Worldwide top 5 found SAP Security research
- Regular presenters on SAP Security
- Developer Protect4S
- Founded in 2010
- Several business partners in BeNeLux

***"ERP-SEC works closely together with SAP to reduce risk in their customers systems. ERP-SEC was invited twice by SAP's global security team in Walldorf to present on their ongoing SAP Security research"***

- Our mission is to raise the level of security of mission-critical SAP platforms with a minimal impact on daily business.

Affiliations: SAP Partner, BIZEC BUSINESS SECURITY, SAP® Certified Powered by SAP NetWeaver®, VNSG

Partners: thenextview++, axl & trax

BSIDES LUXEMBOURG

First of all:

Hat off to Lu hackers

NL

LU

Some next level CTF!!

## Something about SAP

- Market leader in **enterprise** application software
- ~ 300.000 customers worldwide
- SAP customers include:
  - 87% of the Forbes Global 2000 companies
  - 98% of the 100 most valued brands
- Headquarters: Walldorf, Germany, offices in more than 130 countries
- Founded April 1, 1972
- Over 75.000 employees worldwide
- 74% of the world's transaction revenue touches an SAP system
- **Bottomline: Interesting Target!**

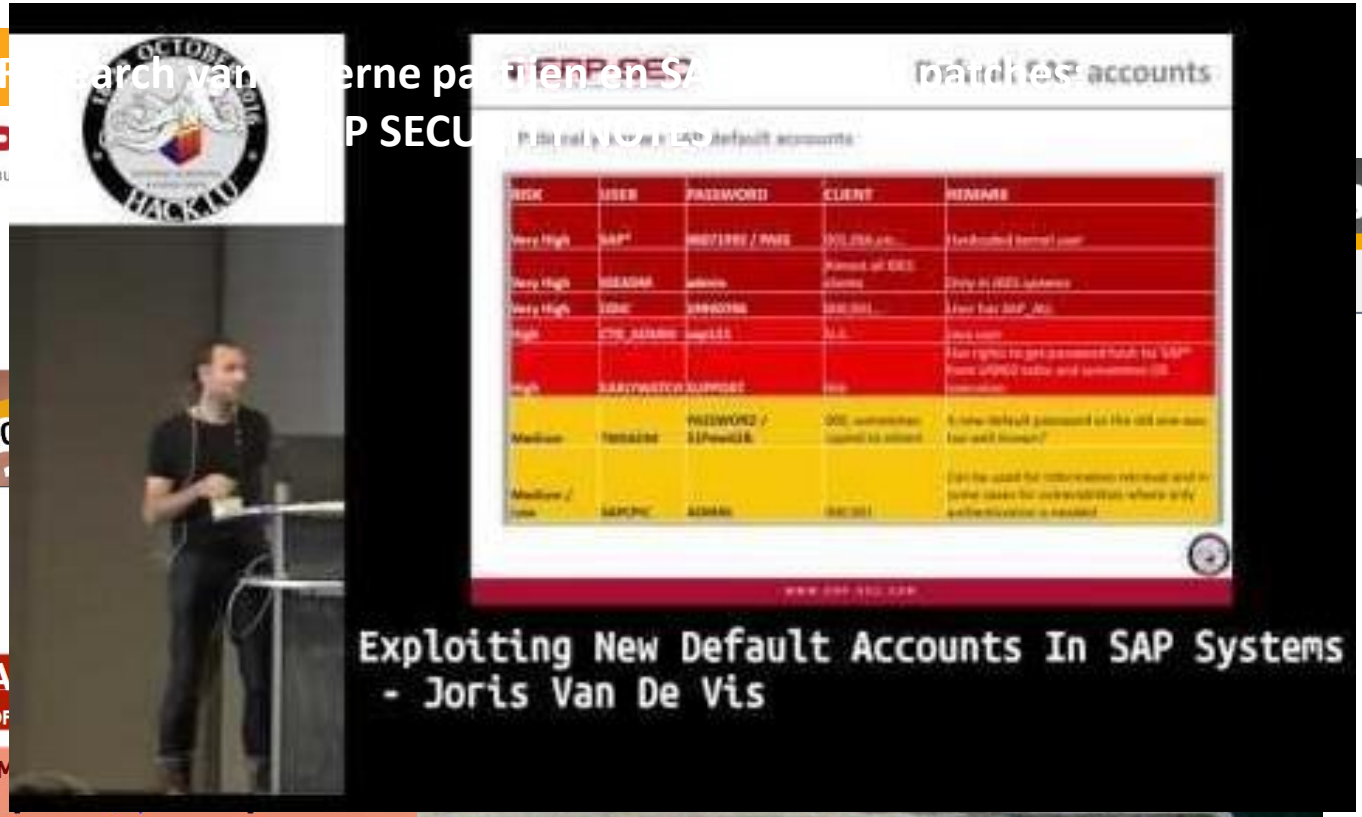

Source: http://www.sap.com/bin/sapcom/en_us/downloadasset.2016-01-jan-26-01.SAP-Corporate-Fact-Sheet-En-20160126-pdf.bypassReg.html

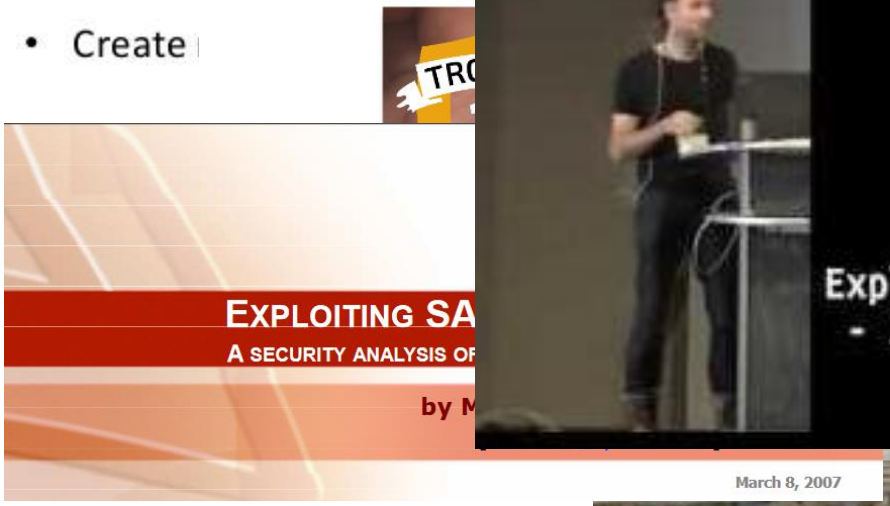
# History SAP Security

**In the beginning…**

- Little focus on security during development of large parts of current ECC, CRM and other systems in the 90's
- SAP Security was all about segregation of duties and critical authorisations
- SAP infrastructure security a blind spot
- SAP takes the topic of Security serious as of 2nd half '00
- Number of discovered vulnerabilities will grow fast throughout the years
- In past 10 years many vulnerabilities discovered by external researchers and SAP in SAP software

# History SAP Security



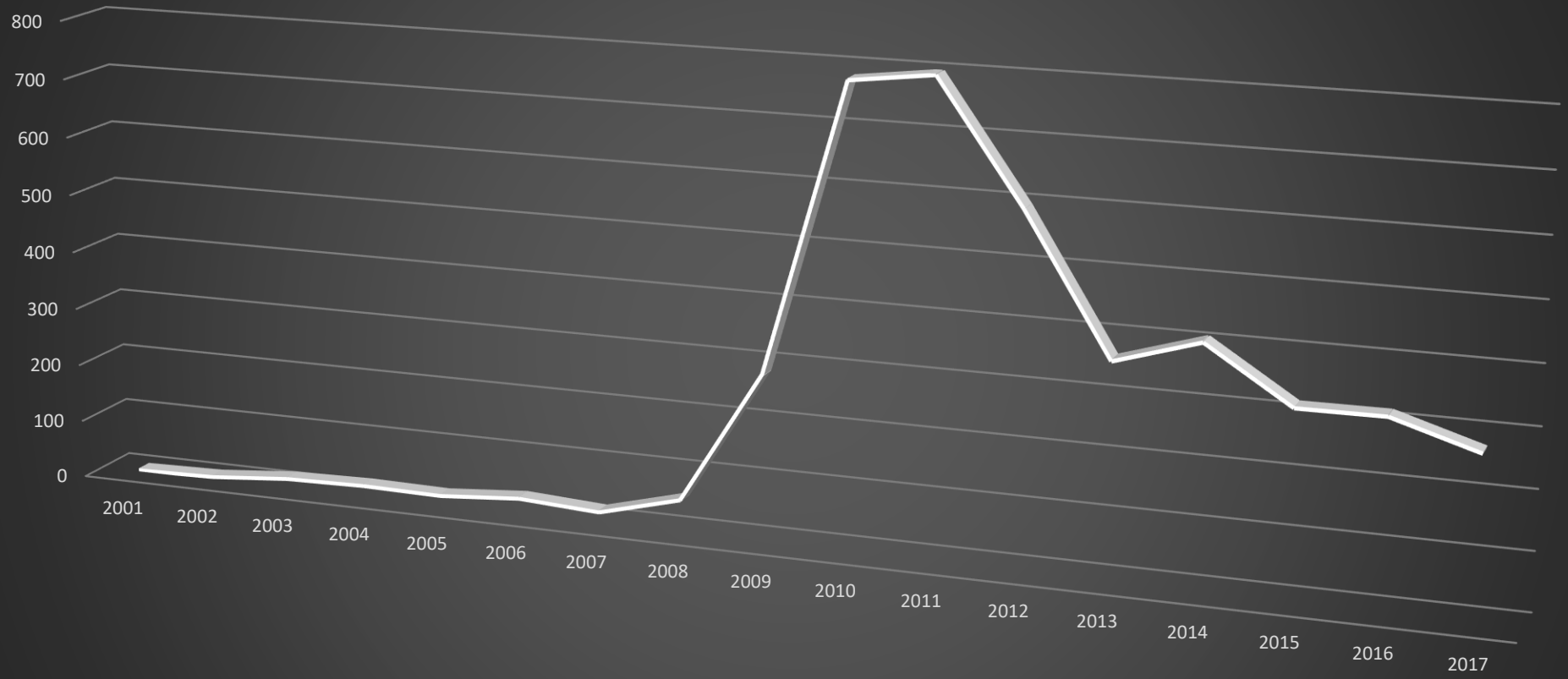





~4000 SAP Security notes

# History SAP Security

## Research of SAP and external researchers had lead to many patches: SAP SECURITY NOTES



# History SAP Security

## Where are we now…

- There is more awareness at SAP customers, but awareness ≠ action
- SAP has improved security, now customers should take action
- Fortune 2000 customers do work on SAP security, but large group stays behind
- GDPR will result in work for most SAP running customers, specific recommendations not clear yet
- Tools exist for detecting vulnerabilities in SAP landscapes, not yet for mitigating them

ERP-SEC
HARMONIZING BUSINESS AND SECURITY

# Up to customers to take action

## Already happening at (mainly large) customers

Customers that do work on SAP CyberSecurity focus on these often found vulnerabilities:

| | Often found High risk vulnerabilities | Risk | Percentage of systems vulnerable |
|---|---|---|---|
| 1 | **Missing (critical) SAP Security notes (GROUPED)** | Very high | 92 |
| 2 | Presence of obsolete or suboptimal password hashes | Very high | 75 |
| 3 | Minimum password length ABAP/JAVA | Very high | 75 |
| 4 | Insecure RFC gateway configuration (GROUPED)*2 | Very high | 63 |
| 5 | Standard users with default passwords (GROUPED)*1 | Very high | 28 |
| 6 | J2EE verb tampering / invoker servlet vulnerable | Very high | 12 |
| 7 | J2EE_ADMIN role / SAP_ALL assigned to wide (GROUPED) | High | 89 |
| 8 | Too many users authorized to perform critical security relevant transactions (GROUPED) | High | 83 |
| 9 | ABAP RFC's with stored login credentials | High | 82 |
| 10 | Is the SAP secure store default key changed*3 | High | 71 |
| 11 | Missing critical Kernel, DB, OS patches (GROUPED) | High | 48 |
| 12 | Is ABAP security log activated | High | 42 |

*1 Default ABAP users, but also DB and for example HANA Root password HP appliances
*2 Multiple vulnerabilities like gw/logging activated, no reg_info or sec_info files or P * * * in ACL's
*3 Hana secure store and ABAP/JAVA secure store combined

BSIDES LUXEMBOURG

ERP-SEC
HARMONIZING BUSINESS AND SECURITY

# Too little, too late?

## Things will go wrong

- 100% prevention imposible, but prevention can and must be done better
- Real-life shows things will go wrong:


BSIDES LUXEMBOURG

# Better safe than sorry

Prevention important to not become a victim too easily
Real-life shows this is not done properly in most cases
Even for trivial items like default passwords and unpatched systems

BLEEPINGCOMPUTER

Search Site

BREAKING: COMMUTERS INJURED AFTER "INCIDENT" AT LONDON TUBE STATION GET ALERTS

NBC NEWS SECTIONS NIGHTLY NEWS MSNBC MEET THE PRESS DATELINE TODAY

BUSINESS › CONSUMER TRAVEL ECONOMY YOUR BUSINESS VEL

BUSINESS
SEP 14 2017, 3:21 PM ET

## Equifax Hackers Exploited Months-Old Flaw

by BEN POPKEN

SHARE
Share
Tweet
Email
Print

Equifax announced late Wednesday that the source of the hole in its defenses that enabled hackers to plunder its databases was a massive server bug first revealed in March.

For the rest of the IT world, fixing that flaw was a "hair on fire moment," a security expert said, as companies raced to install patches and secure their servers. But at Equifax, criminals were able to pilfer data from mid-May to July, when the credit bureau says it finally stopped the intrusion.

Organizations that did a relatively good job at keeping systems patched would have been able to block the attacks. https://www.bleepingcomputer.com/news/security/90-percent-of-companies-get-attacked-with-...

# Out there in real life

Typically seen at customers (no joke)

- Customers apply so called stack upgrade once every year or once every 2 years
- Some do SAP Security notes in between on regular basis (maybe once every 6 months)
- Many do not apply seperate SAP Security notes in between
- SAP Security notes are easy to RE

# There are solutions however

What can be done faster, more easy, better?

- Most time consuming activities are the recurring ones and complex one-time activities
- Activity that stands out → implementing SAP Security notes
- Automate where possible!

# SAP Security notes

## Importance of SAP Security notes

- Contain SAP's corrections to guarantee safety of customers
- Priority from VERY LOW to HOTNEWS
- Regularly releeased on patch Tuesday
- For all SAP products

### Security Notes

Security Notes

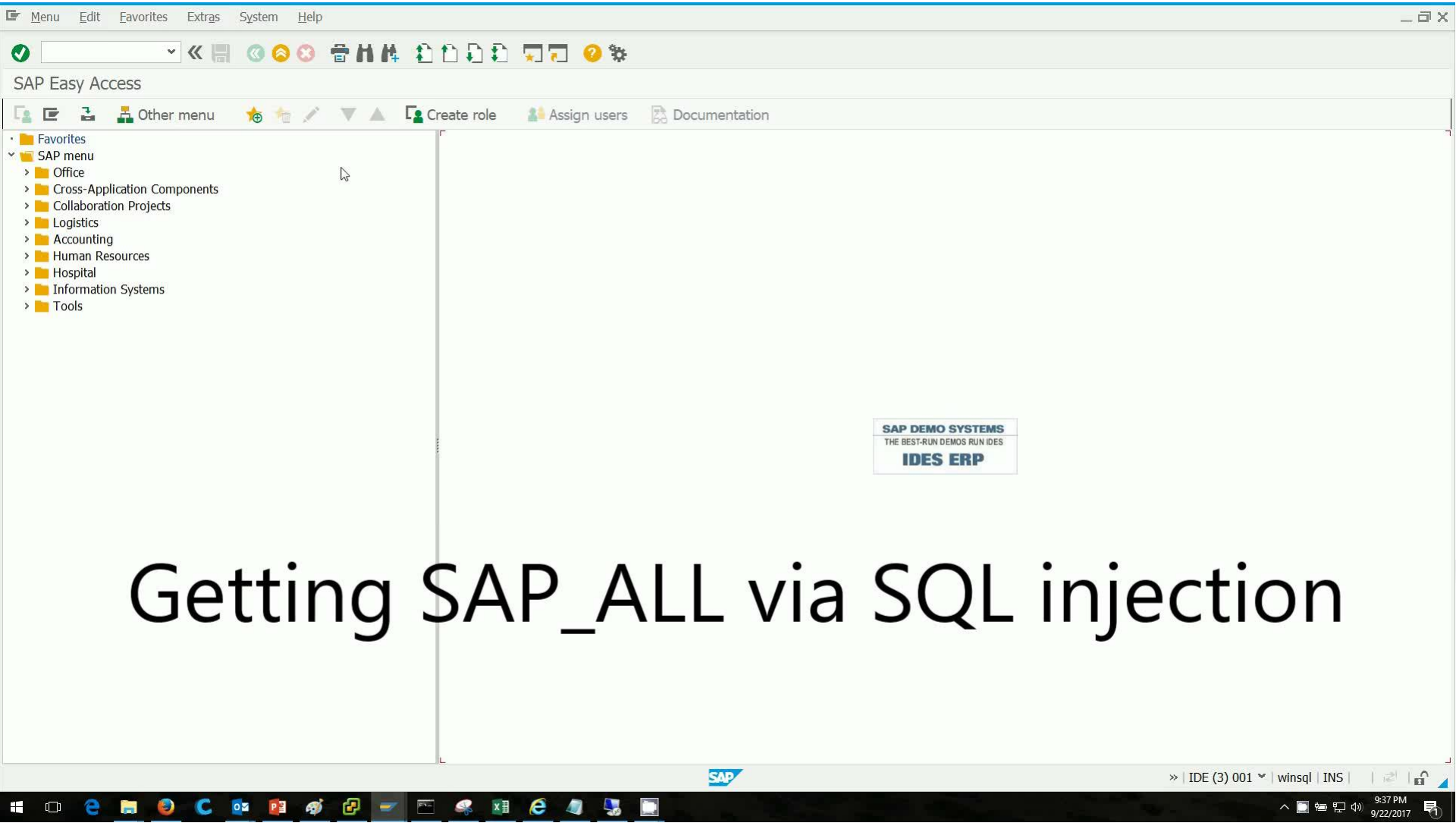
- are standard SAP Notes / HotNews
- with information about known security vulnerabilities
- and appropriate countermeasures (correction instruction, configuration, service pack, upgrade, manual measures)
- whose corrections are contained in subsequently released Support Packages, if possible

https://support.sap.com/content/dam/library/SAP%20Support%20Portal/support-programs-services/support-services/security-optimization-service/media/AGS_Security_Patch_Process.pdf

# SAP Security notes

## A practical example

- One missing SAP Security note can lead to complete compromise of SAP system
- For example via SQL injection from limited account to SAP_ALL
- Solution via SAP Security note 2348055




# Getting SAP_ALL via SQL injection

BSIDES LUXEMBOURG

# SAP Security notes

**Implementing SAP Security notes used to be a lot of manual work.**

According to the SAP Security notes FAQ:

> 16. Can I automatically implement security notes using the application System Recommendation? Is there any remote-implementation function within System Recommendations?
>
> No, you have to implement every security note manually in every DEV-TST-PRD transport landscape. If you are responsible for many DEV systems than you have to implement notes several times.

https://blogs.sap.com/2012/03/27/security-patch-process-faq/

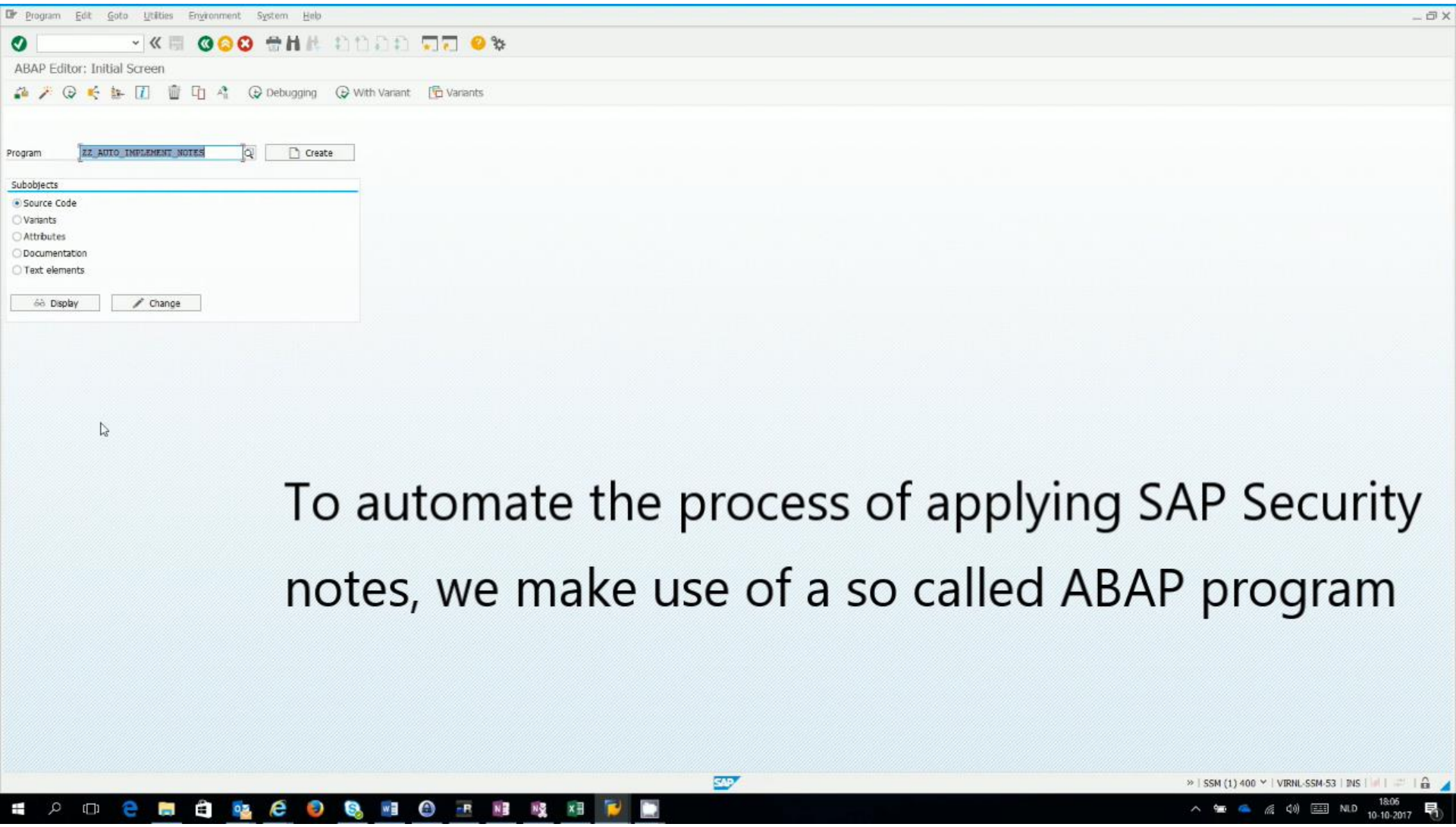
# SAP Security notes

**Manual work, until now:**

To lower the burden of manual, boring, repetitive activities we automated the screen processing of the implementation process.

**Demo: > Apply 50 – 75 % of SAP Security notes automatically**

With ~20-30 SAP Security notes per system each month this used to be a considerable effort.




To automate the process of applying SAP Security notes, we make use of a so called ABAP program

# SAP Security notes

## Business Benefits

- Drastically reduce boring, manual, repetetive activities
- Have better secured SAP systemen (Patch frequentie can be raised)
- Save time
- Have better compliancy

## Concluding

- Riscs of damage or fines grow (GDPR / Internet connected SAP systems)
- Customers need to take action wrt SAP Cybersecurity
- SAP Infrastructures and their security are often complex and cannot be done manually (anymore). Automate this to be effective and efficient
- 1 single missing SAP Security Note canlead to a fully compromised SAP system and all data it contains
- Repetitive mitigation activities wrt SAP Security notes can be automated to some extend to save on time and money and to raise the level of security

ERP-SEC
HARMONIZING BUSINESS AND SECURITY

## For more information see [https://www.protect4s.com](https://www.protect4s.com)


### Protect4S monitors the risks

Data safety is a pressing issue that requires much attention. Protect4S is a uniquely-comprehensive security solution which regularly runs security scans and offers insight into the vulnerabilities that exist in your systems.

### Protect4S scans your entire SAP landscape

It doesn't only scan the application level, but also includes the operating system and database. The data is analysed and vulnerabilities are categorised according to their associated risk levels.

An automatically-generated mitigation report lists the vulnerabilities in order of highest risk level combined with the least time and effort required to resolve the problem. This guarantees the most cost-effective approach to securing your SAP systems.

*"You simply can't afford not to protect your SAP systems and your data"*


BSIDES LUXEMBOURG

ERP-SEC
HARMONIZING BUSINESS AND SECURITY

# Disclaimer

*SAP, R/3, ABAP, SAP GUI, SAP NetWeaver and other SAP products and services mentioned herein as well as their respective logos are trademarks or registered trademarks of SAP AG in Germany and other countries.*

*All other product and service names mentioned are the trademarks of their respective companies. Data contained in this document serves informational purposes only.*

*The authors assume no responsibility for errors or omissions in this document. The authors do not warrant the accuracy or completeness of the information, text, graphics, links, or other items contained within this material. This document is provided without a warranty of any kind, either express or implied, including but not limited to the implied warranties of merchantability, fitness for a particular purpose, or non-infringement.*

*The authors shall have no liability for damages of any kind including without limitation direct, special, indirect, or consequential damages that may result from the use of this document.*

*SAP AG is neither the author nor the publisher of this publication and is not responsible for its content, and SAP Group shall not be liable for errors or omissions with respect to the materials.*



BSIDES LUXEMBOURG

# ERP-SEC

HARMONIZING BUSINESS AND SECURITY

WWW.ERP-SEC.COM