Protect4S
security made simple

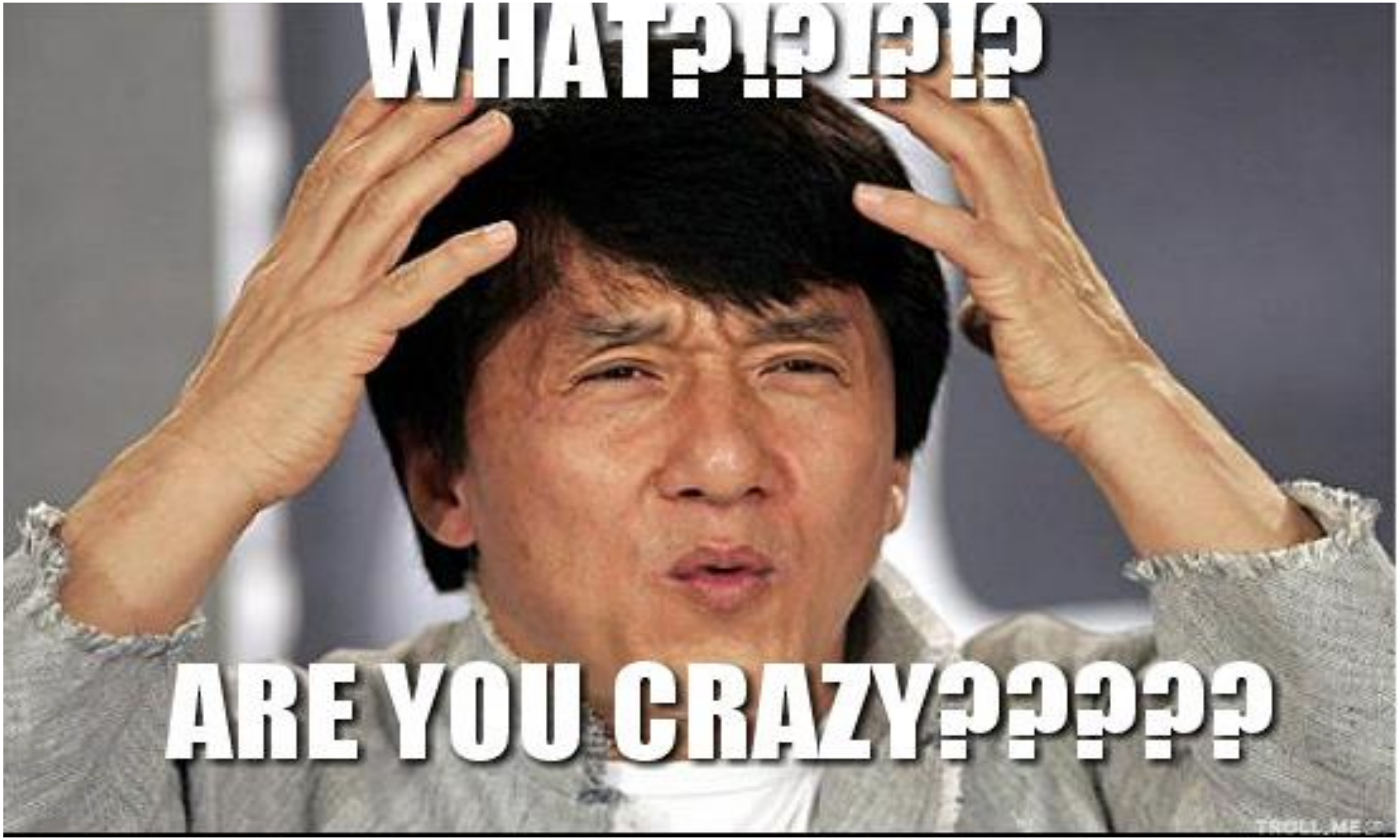
TROOPERS

The importance of

SAP Patch Management

IT-SECURITY CONFERENCE
TROOPERS18

12TH – 16TH MARCH 2018


WHAT?!?!?!?
ARE YOU CRAZY?????
TROLL.ME

ERP Security

"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"

- SAP Security assessments and hardening
- SAP Security research
- Regular presenters on the topic of SAP Security
- Creators of Protect4S
- Founded in 2010

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

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

Some numbers

SAP has released 4000+ security patches to date.

Each month 20+ are added to that number

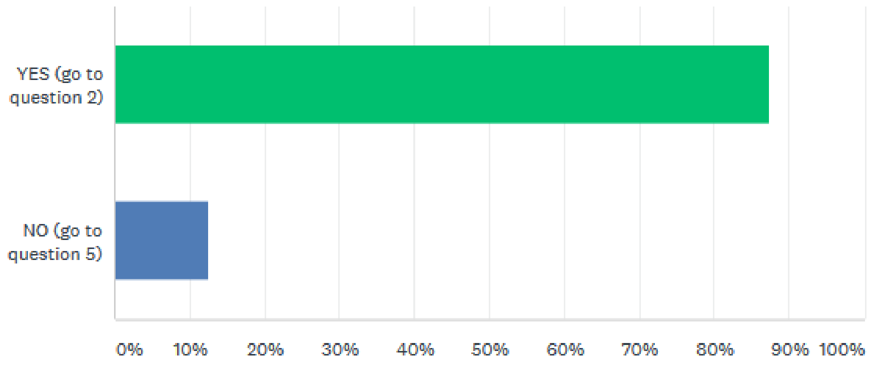
In 2017 alone 268 Security notes were released where 44 have priority HIGH or HOTNEWS

Over 90% of the SAP systems we have assessed over the past 7 years, contained vulnerabilities that could lead to a full compromise. Proper vulnerability management could have prevented this in many cases.

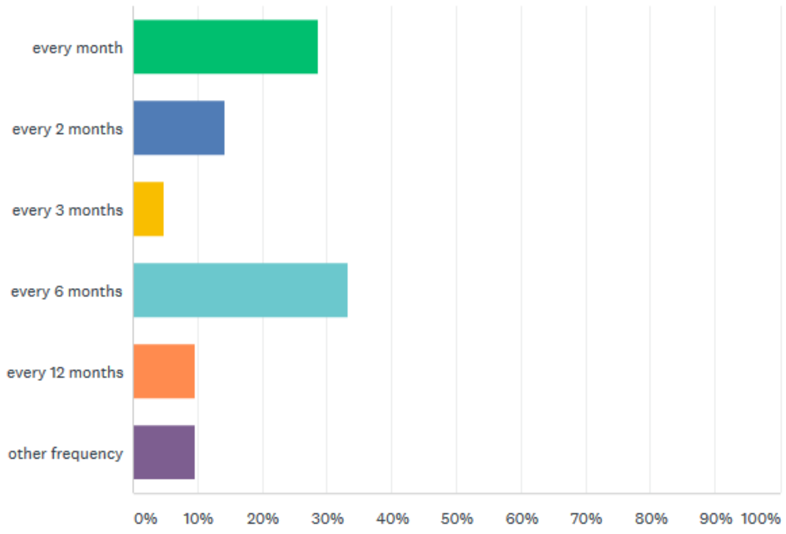
So is this an issue?

- Any SAP customers present here?
- Involved in SAP patching?
- Who implementes SAP Security notes on a monthly basis?
- Who doesn't?

Do you apply SAP Security notes to your SAP systems?



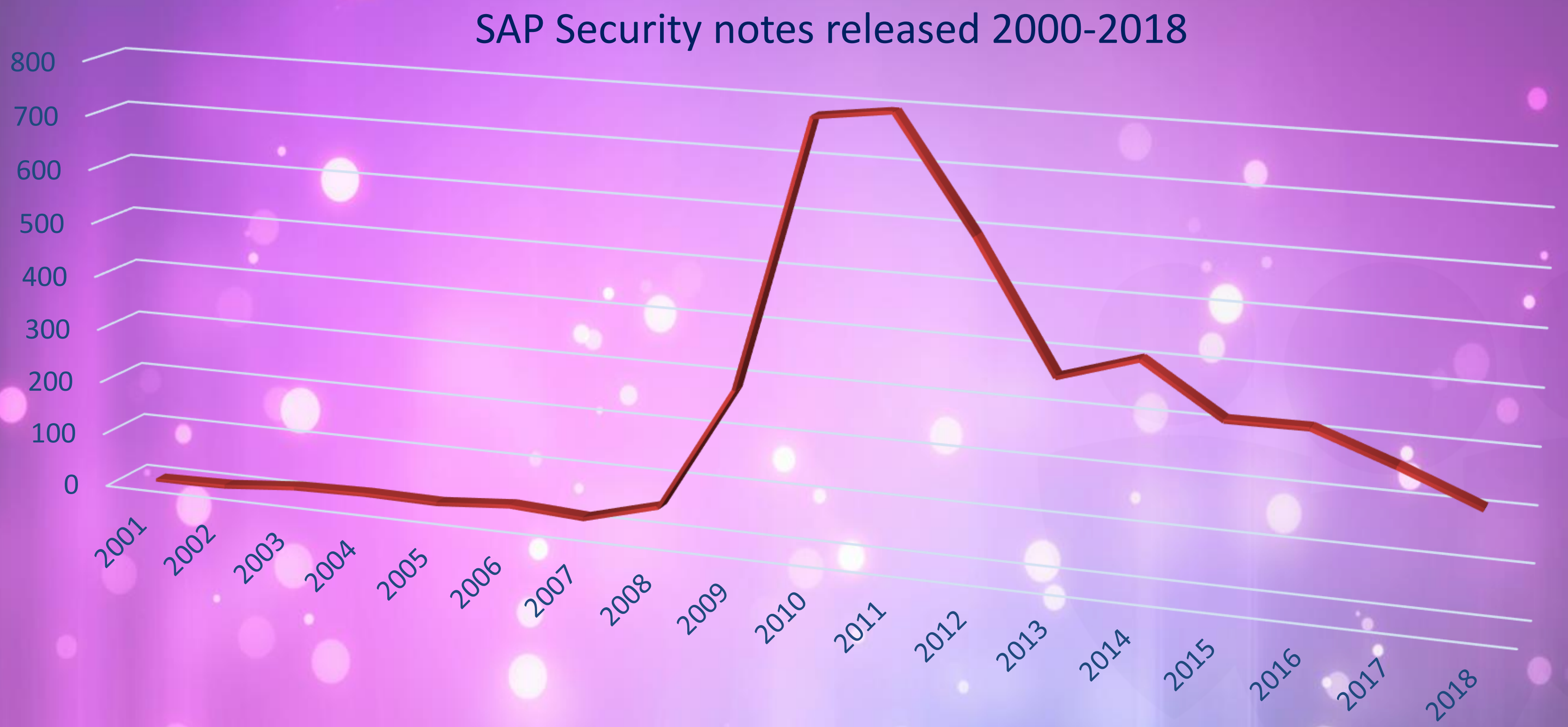
If YES; How regular do you apply SAP Security notes?



Source: Online ERP-SEC survey

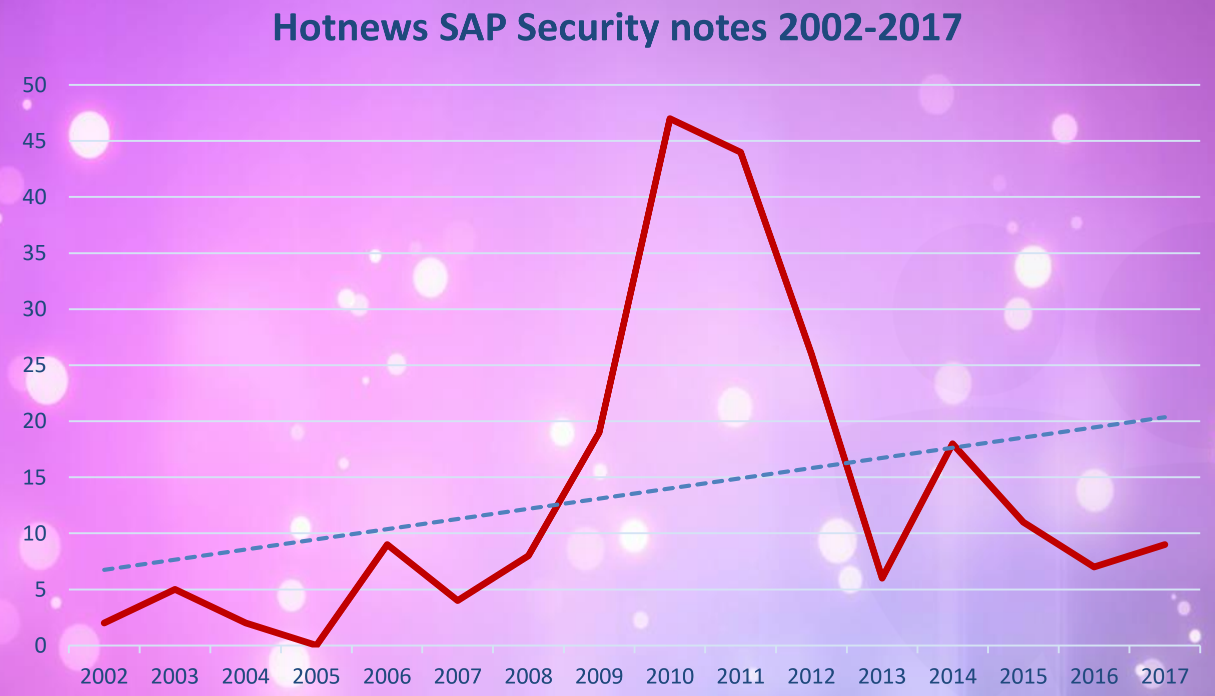
SAP Security notes

Findings of SAP and external researchers resulted in many patches:
> 4000 SAP SECURITY NOTES in total to date



SAP Security notes

SAP Hotnews
Often (unauthenticated) critical vulnerabilities like RCE, SQL injection, OS cmd injection, etc



Demotime – Game Over

Game over…

Demotime

Just 1 missing SAP note…

SAP Patches

SAP note:

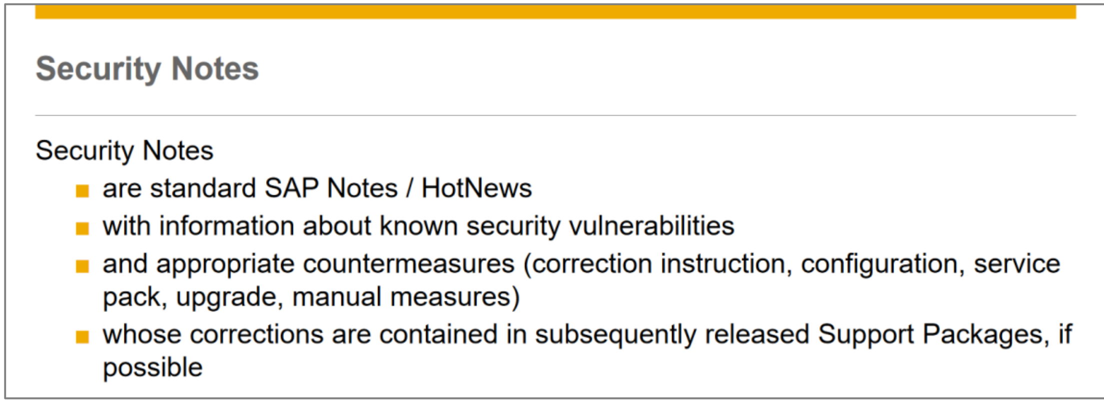
An SAP document on a specific issue. Can be about bugs, new functionality, security or can be informational. Sometimes contains code corrections

SAP security notes:

Notes specifically addressing security issues. Released monthly on patch Tuesday

SAP support package:

Short answer: A collection of bundled SAP notes. Released ~4 times a year



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

SAP Patches

SAP security notes:

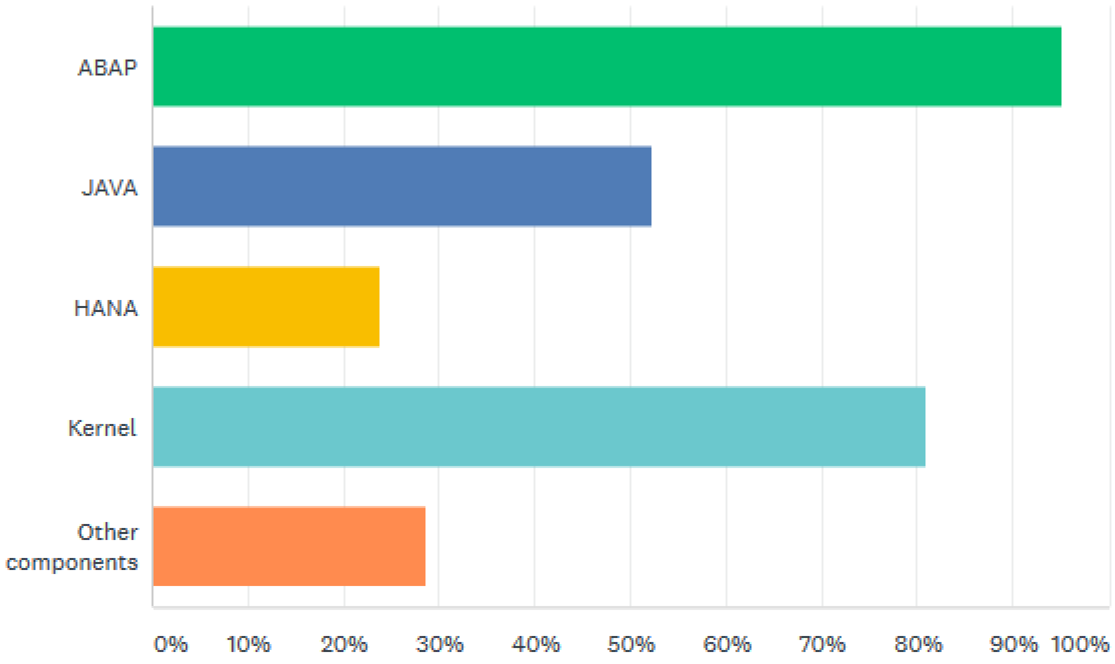
SAP security notes can relate to these components:

- **ABAP stack** (**Vast majority of security notes + most used at customers**)
- Java stack
- SAP kernel
- SAP HANA
- Other components like Business Objects, Databases, etc

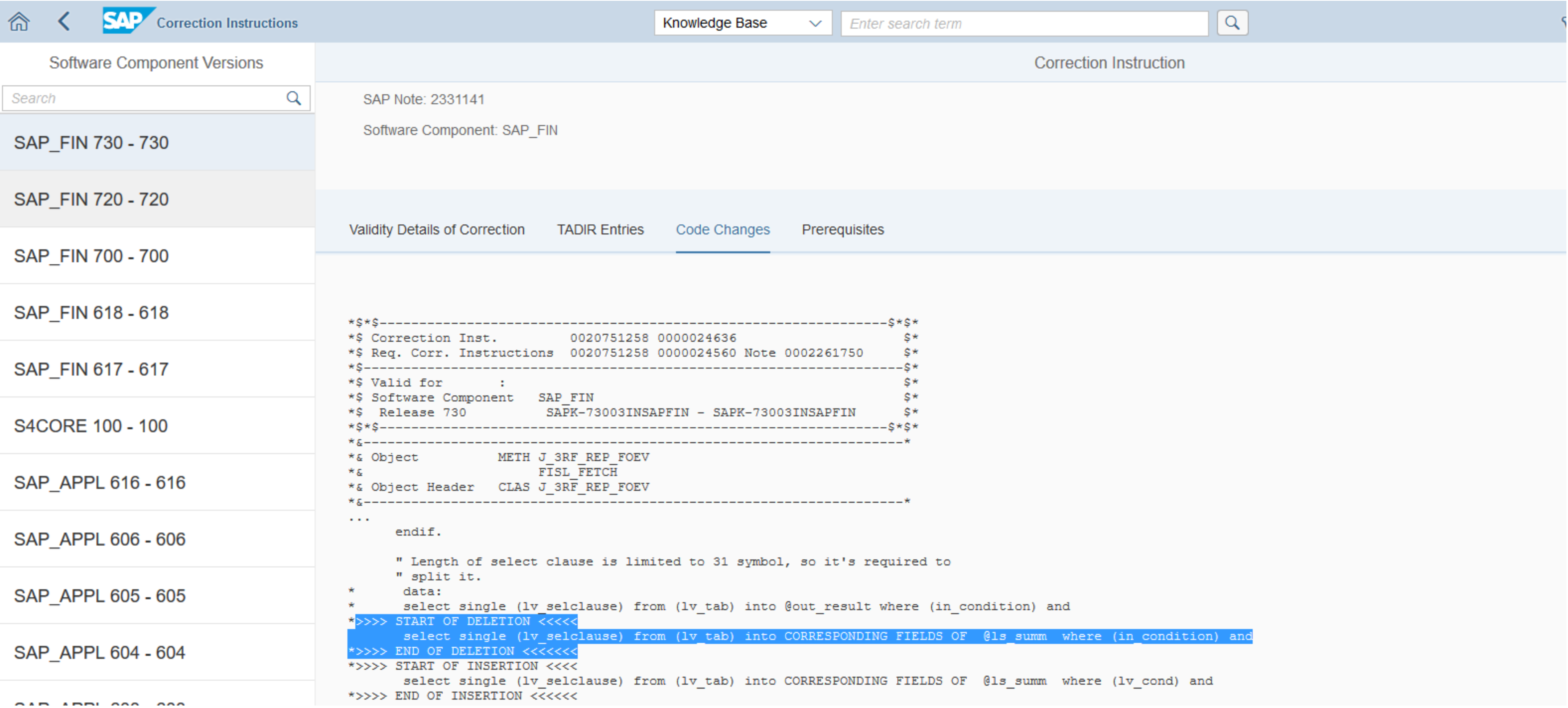
Only ABAP security notes contain code changes. The rest of the notes contain links to patches but no actual code fixes.

SAP Security notes survey

If YES; For which SAP components do you apply SAP Security notes?



Long Risk window



SAP Note: 2331141

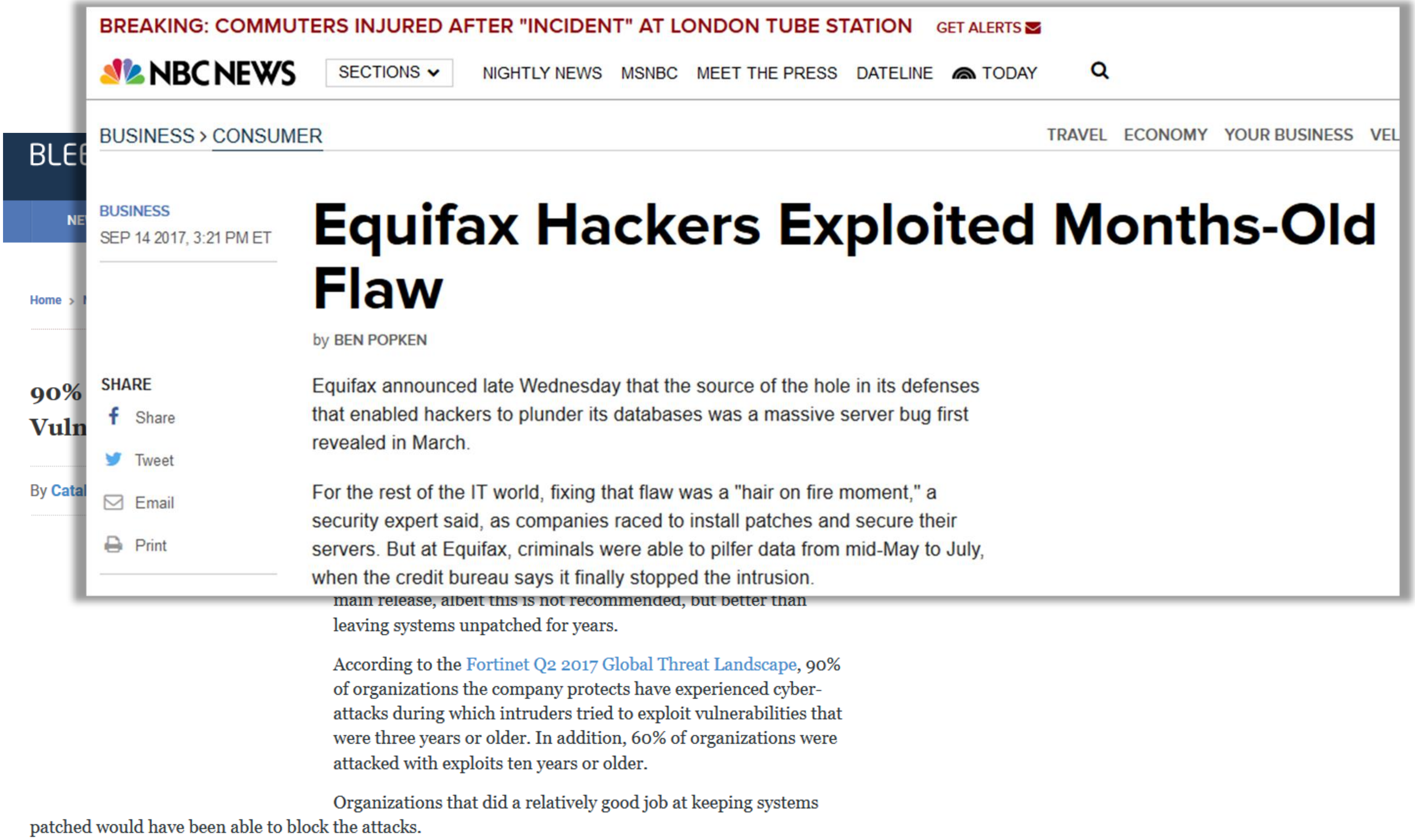
Software Component: SAP_FIN

```
*$*$----------------------------------------------------------------$*$*
*$ Correction Inst.         0020751258 0000024636                     $*
*$ Req. Corr. Instructions  0020751258 0000024560 Note 0002261750     $*
*$--------------------------------------------------------------------$*
*$ Valid for       :                                                  $*
*$ Software Component   SAP_FIN                                       $*
*$  Release 730          SAPK-73003INSAPFIN - SAPK-73003INSAPFIN      $*
*$*$----------------------------------------------------------------$*$*
*&--------------------------------------------------------------------*
*& Object          METH J_3RF_REP_FOEV
*&                      FISL_FETCH
*& Object Header   CLAS J_3RF_REP_FOEV
*&--------------------------------------------------------------------*
...
      endif.

      " Length of select clause is limited to 31 symbol, so it's required to
      " split it.
*      data:
*      select single (lv_selclause) from (lv_tab) into @out_result where (in_condition) and
*>>>> START OF DELETION <<<<<
       select single (lv_selclause) from (lv_tab) into CORRESPONDING FIELDS OF  @ls_summ  where (in_condition) and
*>>>> END OF DELETION <<<<<<<
*>>>> START OF INSERTION <<<<
       select single (lv_selclause) from (lv_tab) into CORRESPONDING FIELDS OF  @ls_summ  where (lv_cond) and
*>>>> END OF INSERTION <<<<<<
```

Protect4S
security made simple

Long Risk window



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

BUSINESS
SEP 14 2017, 3:21 PM ET

Equifax Hackers Exploited Months-Old Flaw

by BEN POPKEN

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.

90%
Vuln

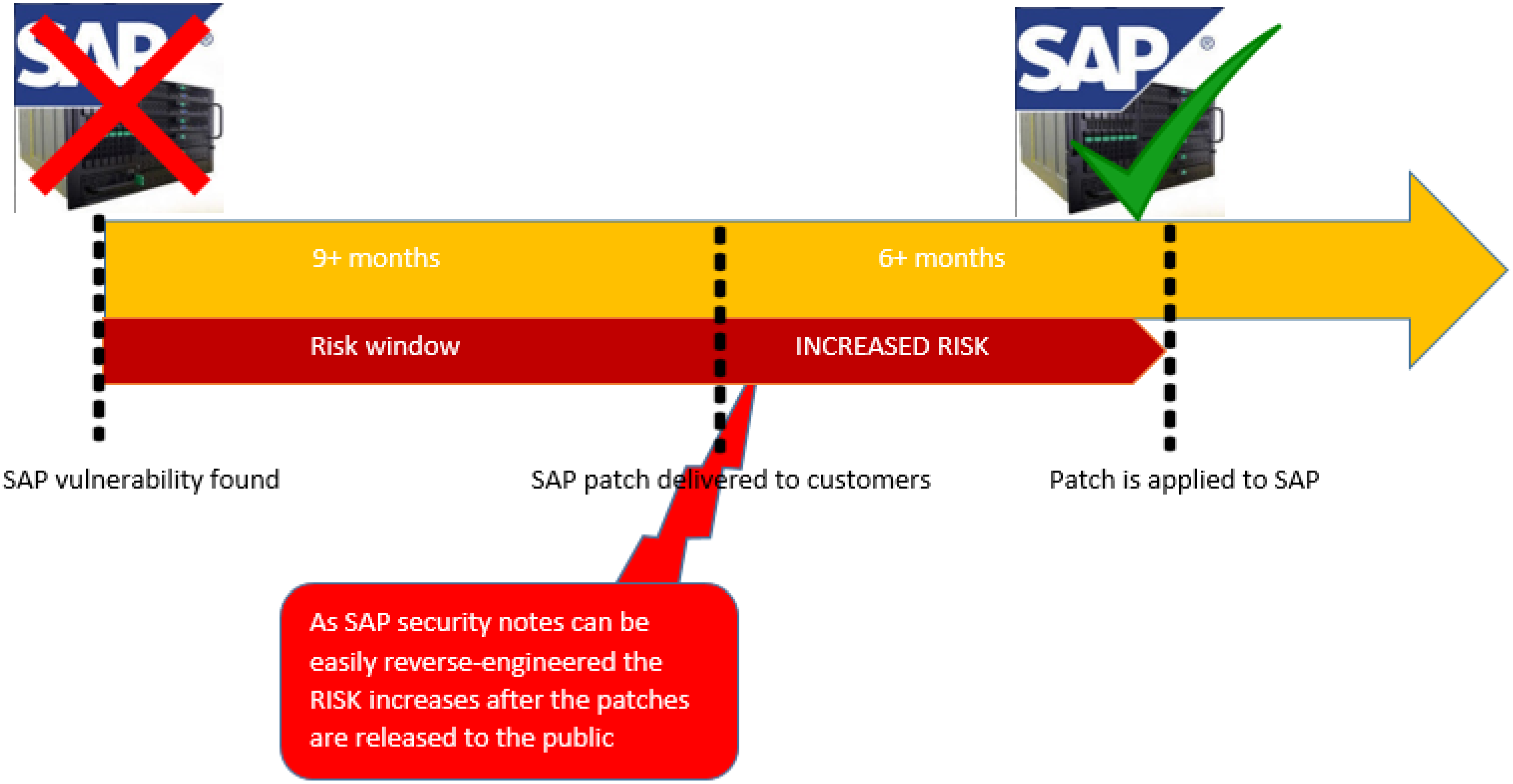
By Catal

main release, albeit this is not recommended, but better than leaving systems unpatched for years.

According to the Fortinet Q2 2017 Global Threat Landscape, 90% of organizations the company protects have experienced cyber-attacks during which intruders tried to exploit vulnerabilities that were three years or older. In addition, 60% of organizations were attacked with exploits ten years or older.

Organizations that did a relatively good job at keeping systems patched would have been able to block the attacks.

Long Risk window



As SAP security notes can be easily reverse-engineered the RISK increases after the patches are released to the public

Some numbers

But what do they mean?

- 42
- 895

Min. number of days it took SAP
to fix one of our >70 reported issues

Max. number of days it took SAP
to fix one of our >70 reported issues

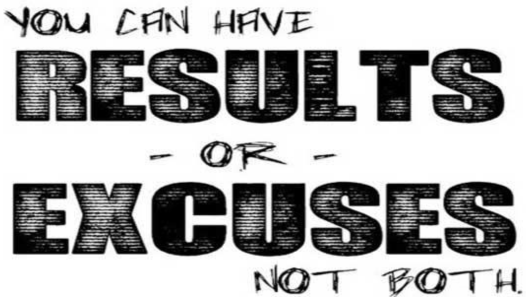
Source: Internal statistics of our own research; over 70 found and reported vulnerabilities

Patch management challenges

Why do SAP customers patch infrequent

- SAP is a **business** system;
    - Functional business changes prioritized higher
    - Patches might break business-critical processes
    - SAP Security notes are bundled with functional releases 3 or 4 times a year
    - Unwanted business downtime can be involved, show must go on
    - Testing typically takes lots of time in these complex systems (if done)
    - Change processes ≠ getting things done

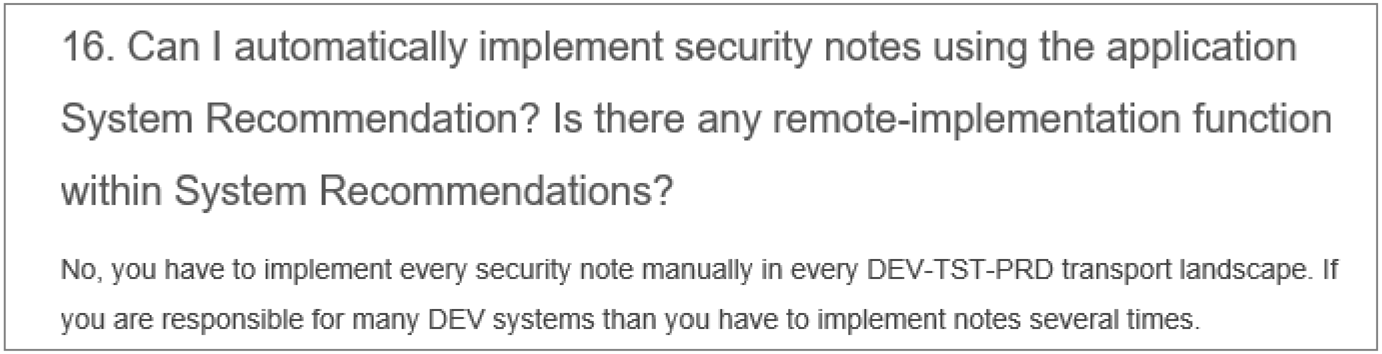
- Awareness of risk still too low on all levels, from SAP basis to architects and business
- Business owners of these systems typically are non-it personnel



Patch management challenges

Why do SAP customers typically patch slow / infrequent (continued)

- Patching
  - Is time-consuming
  - Requires specialist knowledge to judge impact and relevance
  - Is a manual, repetitive, boring task



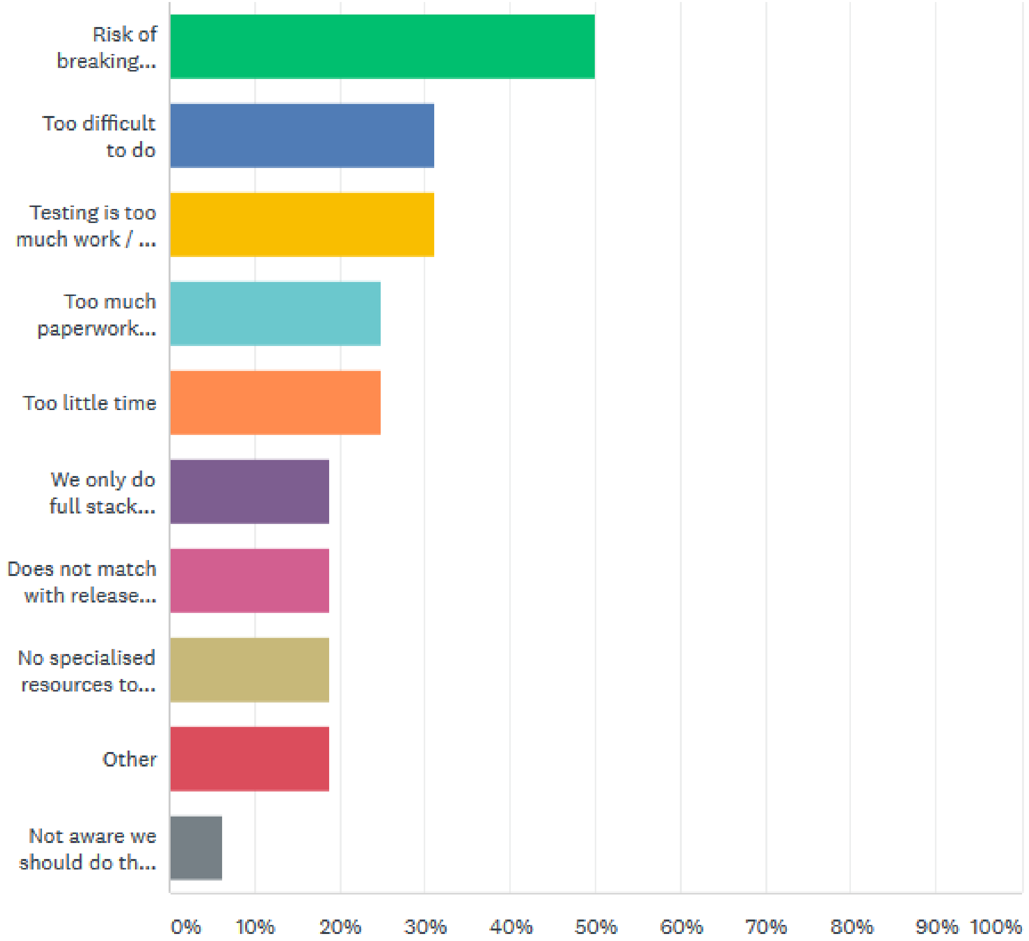
16. Can I automatically implement security notes using the application System Recommendation? Is there any remote-implementation function within System Recommendations?

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 survey

If NOT, why don't you apply SAP Security notes?



There are solutions however

What can be done faster in mitigating? 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!

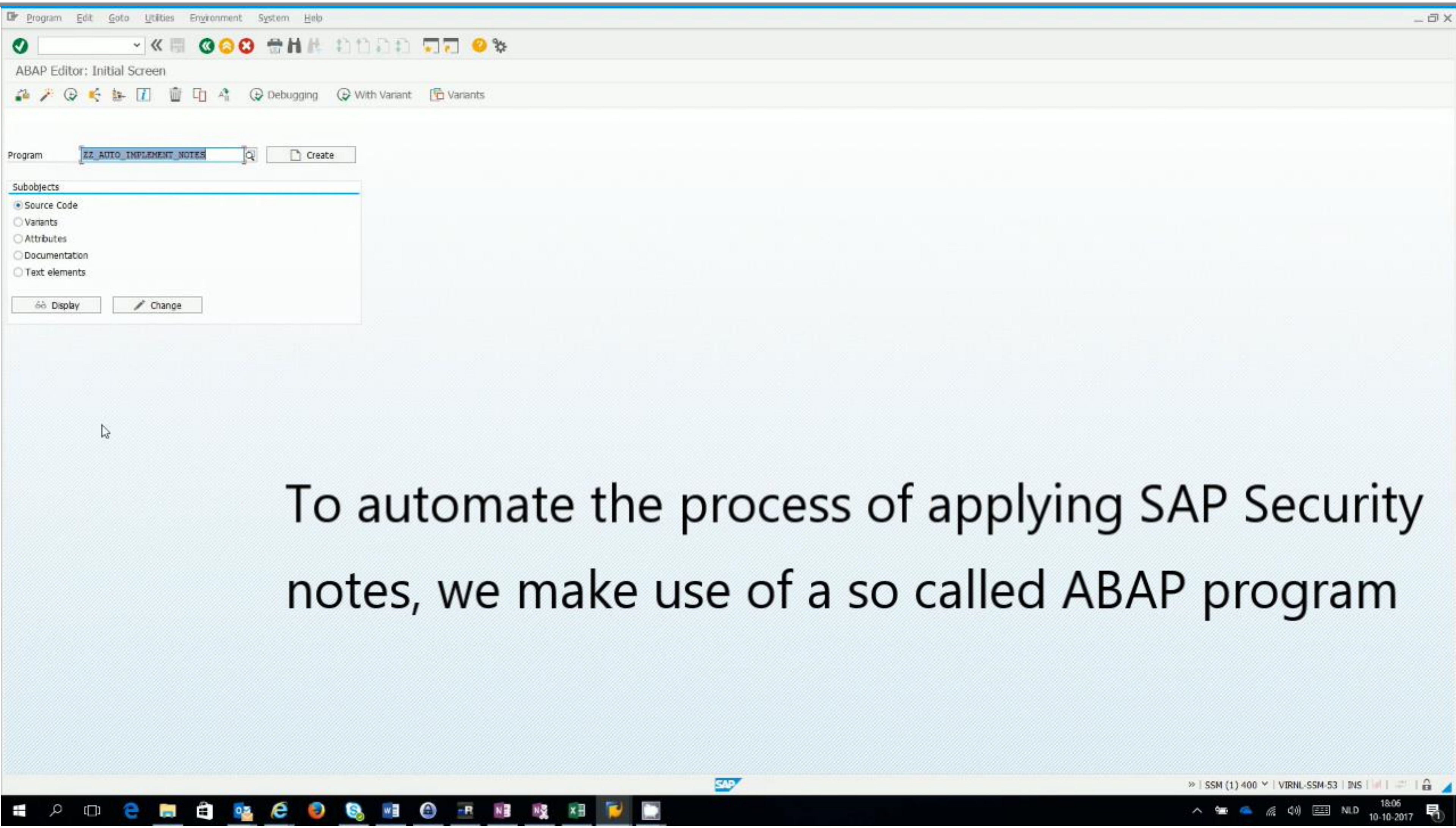
Automate all the things!

Manual work, until now:

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

Customer case demo: > Apply 50 – 75 % of SAP Security notes automatically

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



ABAP Editor: Initial Screen

Program: ZZ_AUTO_IMPLEMENT_NOTES

Subobjects

- ● Source Code
- ○ Variants
- ○ Attributes
- ○ Documentation
- ○ Text elements

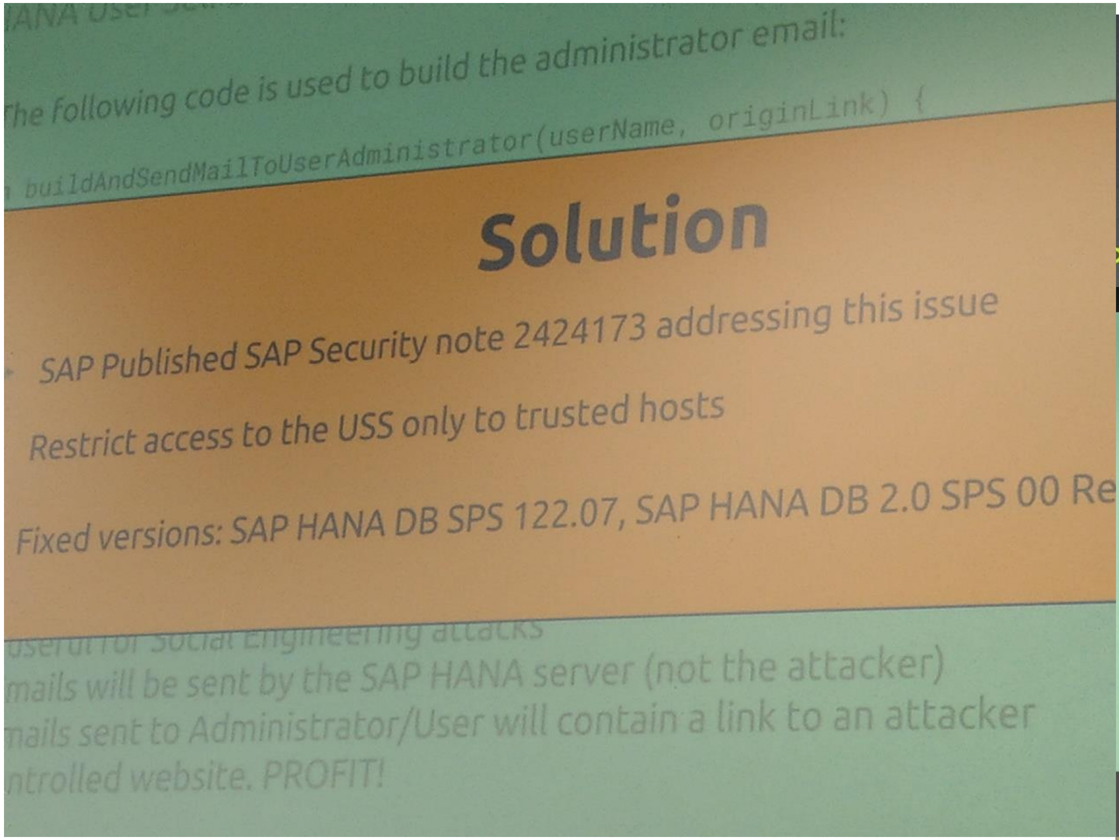
To automate the process of applying SAP Security notes, we make use of a so called ABAP program

Automating SAP Security notes

Business Benefits

- Drastically reduce boring, manual, repetetive activities
- More secure SAP systems (Patch frequentie can be raised)
- Save time
- Better compliancy

Does this look familiar to you?



ANA User Se

The following code is used to build the administrator email:

buildAndSendMailToUserAdministrator(userName, originLink) {

Solution

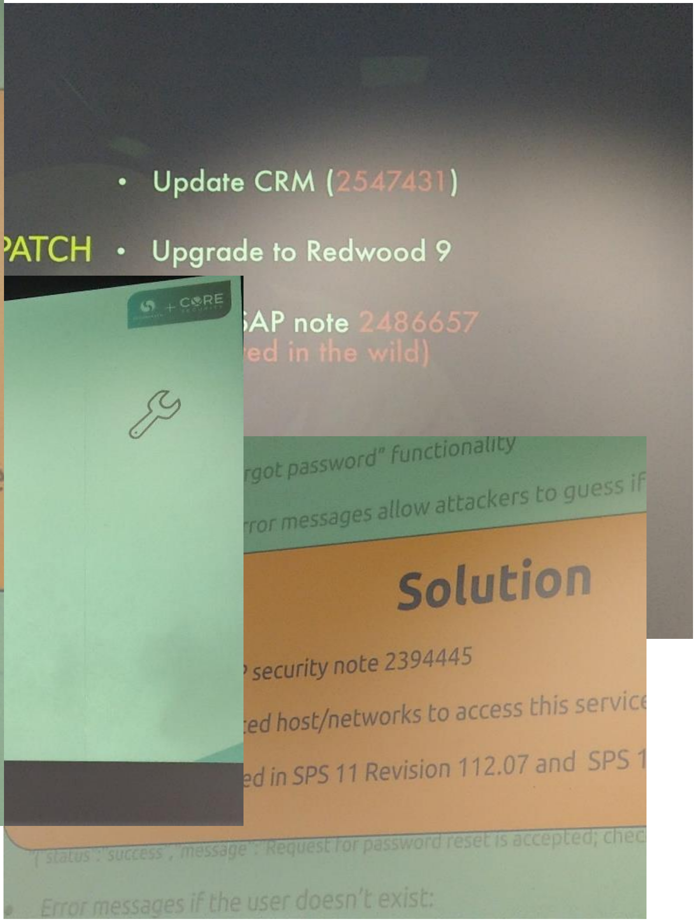
- SAP Published SAP Security note 2424173 addressing this issue
- Restrict access to the USS only to trusted hosts
- Fixed versions: SAP HANA DB SPS 122.07, SAP HANA DB 2.0 SPS 00 Re

useful for Social Engineering attacks

mails will be sent by the SAP HANA server (not the attacker)

mails sent to Administrator/User will contain a link to an attacker

ntrolled website. PROFIT!



- Update CRM (2547431)

PATCH

- Upgrade to Redwood 9
- SAP note 2486657

ed in the wild)

rgot password" functionality

rror messages allow attackers to guess if

Solution

security note 2394445

ed host/networks to access this service

ed in SPS 11 Revision 112.07 and SPS 1

{"status":"success","message":"Request for password reset is accepted; chec

- Error messages if the user doesn't exist:

Troopers #18 SAP track

All presented vulnerabilities and exploits in the Troopers#18 SAP track are solved by SAP Security notes → You know what to do!

Concluding

- SAP has the patches, customers need to take action
- 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 can lead to a fully compromised SAP system and all data it contains
- In order to secure SAP infrastructures do not solely focus on patching, but it can drastically reduce the risks

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.

Protect4S

security made simple

WWW.PROTECT4S.COM

WWW.ERP-SEC.COM