RSAConference2015

Abu Dhabi | 4–5 November | Emirates Palace

CHANGE

Challenge today's security thinking

SESSION ID: SPO-W10B

Anatomy of an Attack

Wolfgang Kandek

Chief Technical Officer
Qualys Inc.
@wkandek

Verizon Data Breach Investigation Report

2122 Data Breaches

Financial data, Product data, Personal data, Usernames/Passwords

Vulnerabilities

> 99% over 1 year old

Demo

Vulnerabilities

Patch

95%/99%

Softwareprodukte

- Adobe Flash Player
- Adobe Reader
- Apple OS X
- Apple Quicktime
- Apple Safari
- Google Chrome
- Linux Kernel
- Microsoft Internet Explorer
- Microsoft Office
- Microsoft Windows
- Mozilla Firefox
- Mozilla Thunderbird
- Oracle Java/JRE

Tabelle 1: Auswahl von Softwareprodukten mit hoher Relevanz

Vulnerabilities

Patch

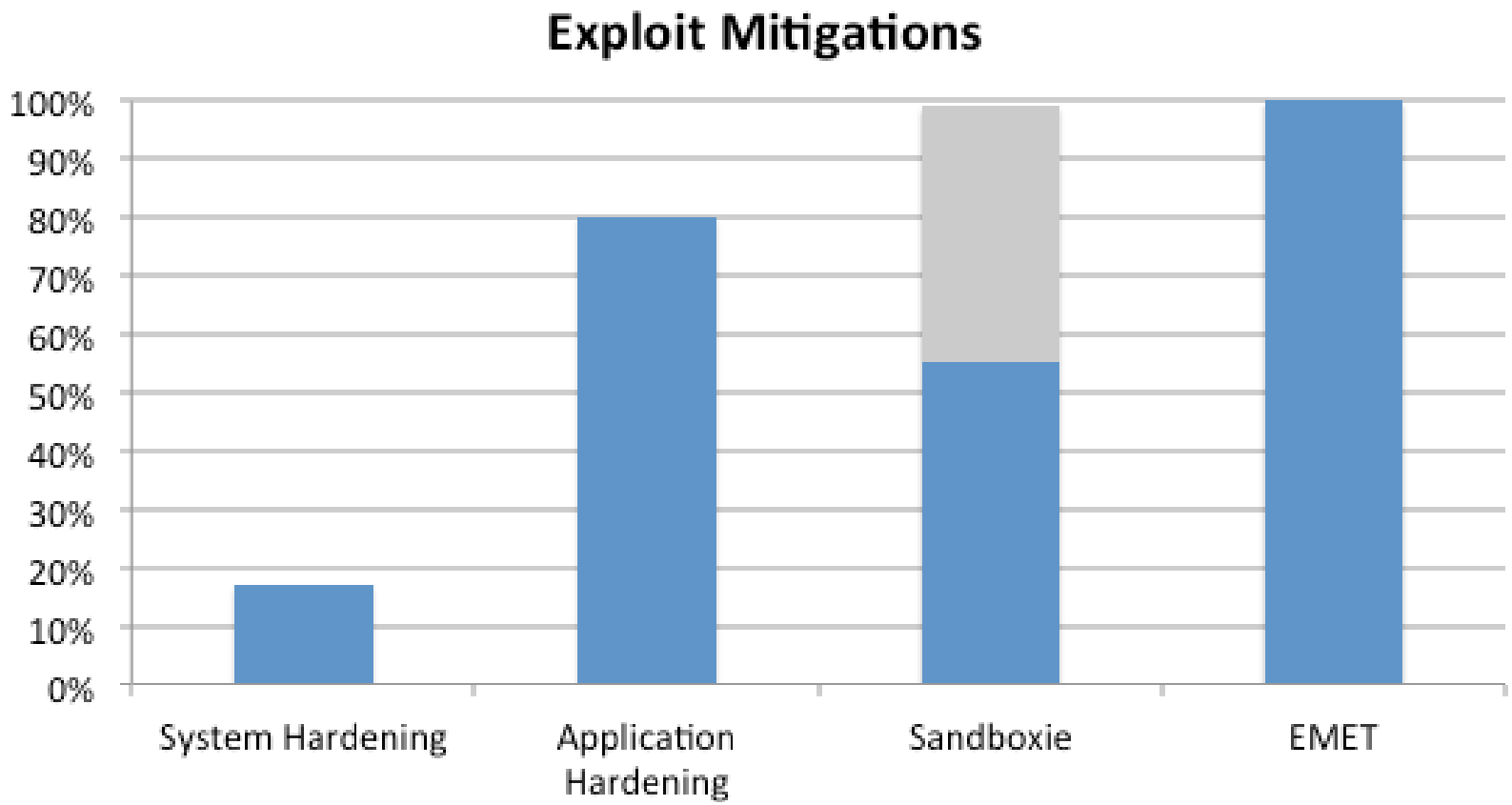
95%/99%

Priority on Exploits

MS15-020, MS15-051

0-days

Hardening


Exploit Mitigations
100%
90%
80%
70%
60%
50%
40%
30%
20%
10%
0%
System Hardening
Application Hardening
Sandboxie
EMET

Then:

Passwords

Finally:

Breach Detection

What can you do now?

- Next 30 days:
  - Inventory of Devices
  - Inventory of Software
- Next 60 days - Vulnerability Assessment
- 90 days: Patch Plan and Execute
- In parallel: Password Quality and 2-factor

RSAConference2015

Abu Dhabi | 4–5 November | Emirates Palace

Thank you

Wolfgang Kandek
wkandek@qualys.com
@wkandek

http://www.qualys.com

Resources

- Verizon DBIR 2015
  http://www.verizonenterprise.com/DBIR/
- Chevron
  https://www.rsaconference.com/events/us15/agenda/sessions/1983/building-a-next-generation-security-architecture
- BSI
  https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2014.pdf
- Hardening
  https://www.virusbtn.com/pdf/conference_slides/2013/Niemela-VB2013.pdf