The human factor in ICS
Why is it important to create awareness?
About me – Daniel Buhmann

- Business Unit Manager Security Solutions at KORAMIS GmbH
- Industrial IT Security old-timer (since 13 years)
- Computer Scientist with Digital Media background moving to (Industrial) IT Security
Basics

ETERNALBLUE
∞
8.03 M
network devices vulnerable

HEARTBLEED
90 M
network devices vulnerable

SHELLSHOCK
70%
of all Internet-facing machines exposed

STAGEFRIGHT
Billion
Android devices possibly affected by major flaw in Media Library

EFAIL
vulnerabilities in the end-to-end encryption technologies

DIRTY COW
Almost every Linux based system vulnerable due to privilege escalation bug

FLASH
Almost every Linux system vulnerable due to glibc flaw

WINDOWS
Numerous remote code execution vulnerabilities discovered
"Only amateurs attack machines; professionals target people"

- Bruce Schneier, Cryptographer (2000)
Our CEO got spearphished!

What? We bought IPS, IDS, DLP, HIPS, WAF, NGFW, IOCs, AV, anti-APT appliances

Did they use ROP? How did they bypass CFG, ASLR, EMET, EAF, DEP, SEHOP, SafeSEH, GS, and win32k syscall disabling?

It was a Word doc with a macro

That wasn't in any of our Magic Quadrant reviews...
A universe of interactions dark to your billion dollar security solutions

- security events and alerts
- logs and configuration data
- user and network activities

- talking with customers
- talking with family and friends
- writing down information as reminder
- etc.

traditional security data

human generated actions
Productivity in Night Shifts
Media vs Security
Removeable Media
Game Plan

Drop 297 USB keys and see what happens

<table>
<thead>
<tr>
<th></th>
<th>Total</th>
<th>Fraction</th>
</tr>
</thead>
<tbody>
<tr>
<td>Key dropped</td>
<td>297</td>
<td></td>
</tr>
<tr>
<td>Key picked up</td>
<td>290</td>
<td>98%</td>
</tr>
<tr>
<td>Key who phoned home</td>
<td>135</td>
<td>45%</td>
</tr>
<tr>
<td>Key returned</td>
<td>54</td>
<td>19%</td>
</tr>
<tr>
<td>People answering survey</td>
<td>62</td>
<td>21%</td>
</tr>
</tbody>
</table>

source: Elie Bursztein – blackhat 2016
Ooops, your files have been encrypted!

What Happened to My Computer?
Your important files are encrypted. Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?
Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.
You can decrypt some of your files for free. Try now by clicking <Decrypt>.
But if you want to decrypt all your files, you need to pay.
You only have 3 days to submit the payment. After that the price will be doubled. Also, if you don’t pay in 7 days, you won’t be able to recover your files forever.
We will have free events for users who are so poor that they couldn’t pay in 6 months.

How Do I Pay?
Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.
Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.
And send the correct amount to the address specified in this window.
After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am GMT from Monday to Friday.

Send $600 worth of bitcoin to this address:
13AM4VW2dhxYgXeQepoHkJHSQwy6NgaE94

Copy

Contact Us
IBM workers banned from using USB sticks

Staff at IBM have been banned from using removable memory devices such as USB sticks, SD cards and flash drives.

The ban could cause "disruption" to work habits, warned IBM.

The possibility of "financial and reputational" damage if staff lost or misused the devices prompted the decision, reported The Register.
O’zapft is
People

% of businesses where employees hide cybersecurity incidents (by segments)

- VSB (1 to 49): 29%
- SMB (50 to 999): 42%
- Enterprise (1000+): 45%

source: Kaspersky IT Security Risks Survey 2017, global data
Credentials

“81% of hacking-related breaches leveraged either stolen and/or weak passwords.”

DATA BREACH STATISTICS
DATA RECORDS LOST OR STOLEN SINCE 2013

9,727,967,988

ONLY 4% of breaches were “Secure Breaches” where encryption was used and the stolen data was rendered useless.

DATA RECORDS ARE LOST OR STOLEN AT THE FOLLOWING FREQUENCY

<table>
<thead>
<tr>
<th>Frequency</th>
<th>Records</th>
</tr>
</thead>
<tbody>
<tr>
<td>EVERY DAY</td>
<td>4,960,718</td>
</tr>
<tr>
<td>EVERY HOUR</td>
<td>206,697</td>
</tr>
<tr>
<td>EVERY MINUTE</td>
<td>3,445</td>
</tr>
<tr>
<td>EVERY SECOND</td>
<td>57</td>
</tr>
</tbody>
</table>

';--have i been pwned?
Check if you have an account that has been compromised in a data breach

sources: Verizon, haveibeenpwned.com, breachlevelindex.com
Oh no — pwned!
This password has been seen 20,833 times before

This password has previously appeared in a data breach and should never be used. If you've ever used it anywhere, SCREW IT and change it!

Choose a word that's already in your heart. Like "Nutella", for example! #WorldPasswordDay #Nutella pic.twitter.com/Q9EERc6244

130 gefällt   95 Retweets
Invest for awareness

safety

security
Effective learning

source: The Infosec Institute
Monitor effectiveness

Great!
Only 3 failures out of 100—well within the 95% threshold

source: Kipper Williams
audience.ask(questions);
That’s it!

Daniel Buhmann
Business Unit Manager Security Solutions

d.buhmann@koramis.de
Phone:  +49 681 968191 11
Fax:  +49 681 968191 911
Mobile:  +49 151 18483752