

10 Deadly Sins of Administrators about Windows Security



Paula Januszkiewicz

CQURE: CEO, Penetration Tester; Cybersecurity Expert

CQURE Academy: Trainer

Microsoft Regional Director

MVP: Enterprise Security, MCT

www.cquireacademy.com

paula@cquire.us



@paulacquire
@CQUREAcademy

What does CQURE Team do?

Consulting services

- **High quality penetration tests** with useful reports
 - Applications
 - Websites
 - External services (edge)
 - Internal services
 - + configuration reviews
- **Incident response** emergency services
 - immediate reaction!
- **Security architecture and design advisory**
- Forensics investigation
- Security awareness
 - For management and employees

Trainings

- Security Awareness trainings for executives
- CQURE Academy: over 40 advanced security trainings for IT Teams
- Certificates and exams
- Delivered all around the world only by a CQURE Team: training authors

info@cquire.us



IMPORTANT UPDATE If You Want To
Seriously Level Up In This Area...

Featured TechEd 2012 Speakers [More featured speakers →](#)



Wally Mead



John Craddock



Mark Russinovich



Paula Januszkiewicz

Microsoft

CQURE X ACADEMY[©]



We are proud to announce that
Paula Januszkiewicz
was rated as
No 1 Speaker
at Microsoft Ignite!!!

May 4-8, 2015
Chicago, IL



No.1 Speaker

Paula Januszkiewicz
CEO CQURE

She received
a "Best of Briefings" award at her
"CQTools: The New Ultimate Hacking Toolkit"
Black Hat Asia 2019 briefing session

black hat



ATTEND TRAININGS BRIEFINGS ARSENAL FEATURES SCHEDULE SPECIAL EVENTS

SEE ALL PRESENTERS

SPEAKER



PAULA JANUSZKIEWICZ
CQURE INC.

Paula Januszkiewicz is a CEO and Founder of CQURE, also an Enterprise Security MVP and a well-known speaker to customers all around the world. She has a deep belief that positive thinking is key to success and pays extreme attention to details and conference content.


Brian Keller


Paula Januszkiewicz



Mark Minasi



John Craddock



Scott Woodgate



Marcus Murray

General Sessions Applications and Development Cryptography and Architecture Hackers and Threats Mobile and Network Security Trusted and Cloud Computing


Mark Kennedy
Symantec
Topic: Anti-Malware Industry... Cooperating. Are You Serious?


Samir Saklikar
Dennis Moreau
RSA, The Security Division of EMC
Topic: Big Data Techniques for Faster Critical Incident Response


Marc Bown
Trustwave
Topic: APAC Data Compromise Trends


Paula Januszkiewicz
CQURE
Topic: Password Secrets Revealed! All You Want to Know but Are Afraid to Ask

the adventures of alice & bob

论坛
Forum
2011

Where The World Talks Security
November 2 - 3
China World Hotel
Beijing, China

Registration & Accommodation Agenda & Sessions Sponsors Contact Us

Thursday, November 3



Technical systems are:
Reviewed
Scanned
Penetration Tested

So?

And here come statistics...

BUSINESSES BREACHED THAT *DID NOT* HAVE
SECURITY POLICIES IN PLACE THAT INCLUDED
SECURITY
AWARENESS
EDUCATION
PROGRAMS

87%

IT PROFESSIONALS THAT REPORT SECURITY
POLICIES ARE COMMUNICATED TO NEW
HIRES DURING
ORIENTATION

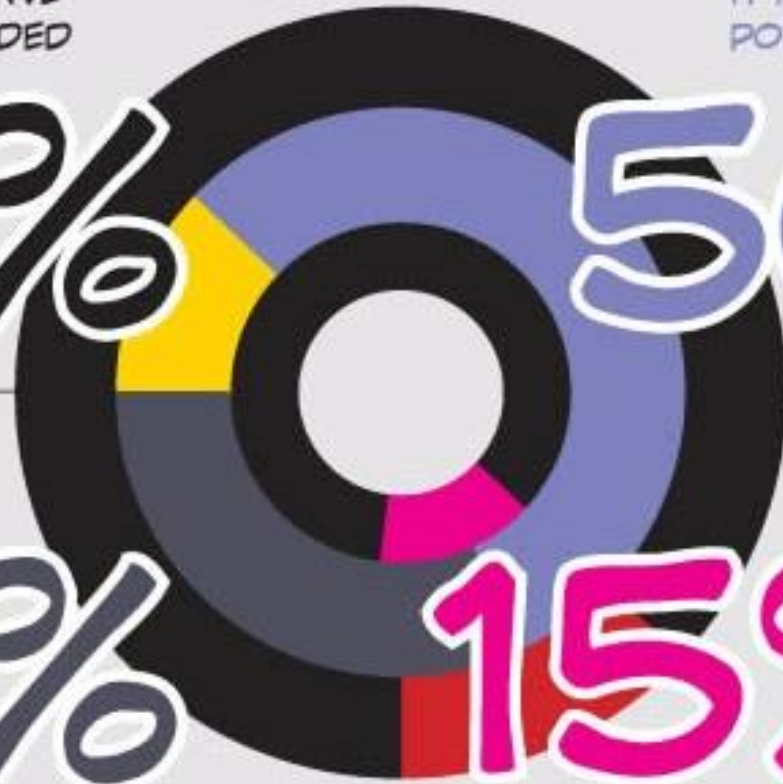
56%

EMPLOYEES THAT SAY
THEY WERE
EDUCATED
ON SECURITY
POLICIES

32%

15%

PUBLICLY REPORTED
INSIDER BREACHES
THAT ARE EXECUTED WITH
MALICIOUS INTENT



Awareness >> Behavior >> Culture

Each organization processing sensitive data **must aim**
for a responsible security culture.

Awareness comes with experience



Issue No.

Fee

Rem
Type

O/D

S/C

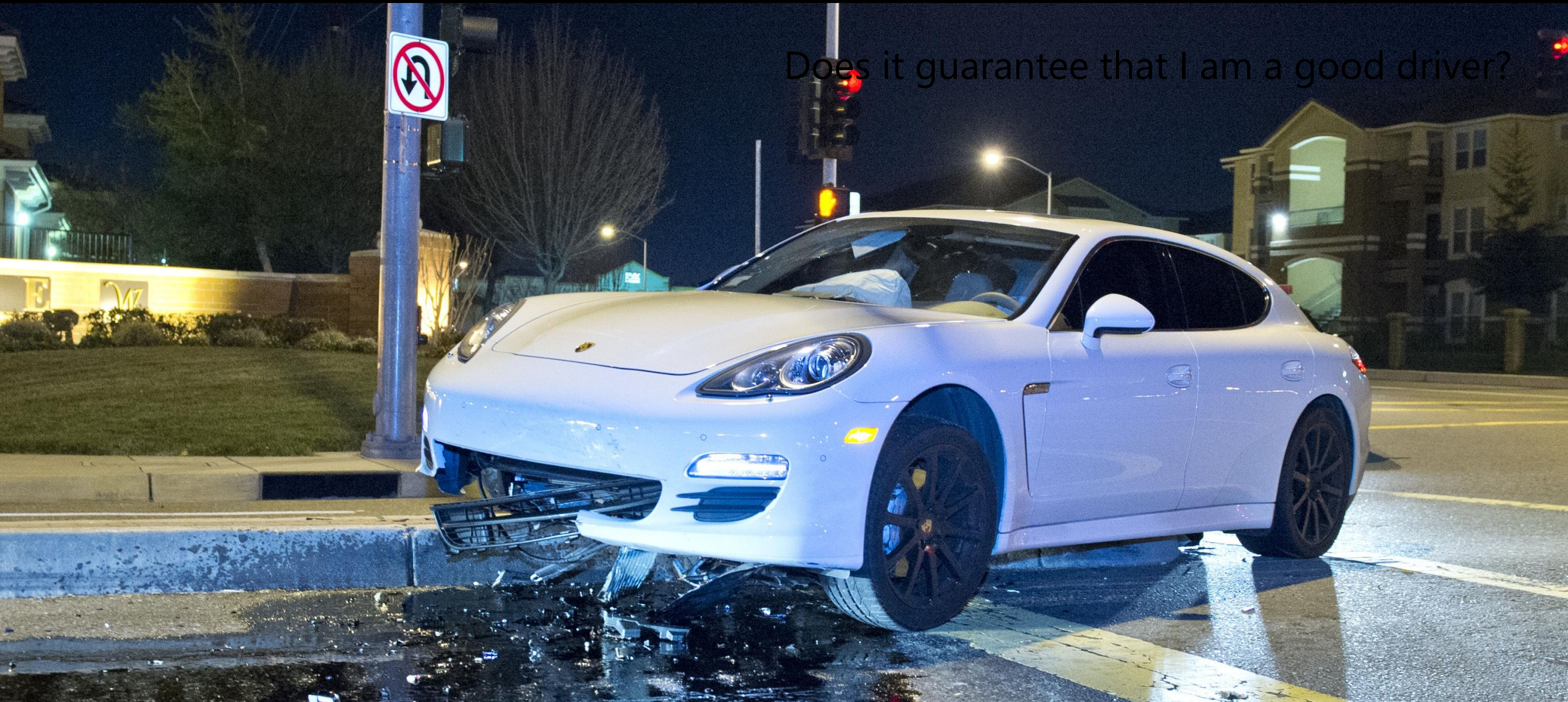
T/P

I know the traffic rules....

PRACTICAL DRIVING TEST PASS CERTIFICATE

This is to certify that:

Behavior comes with awareness



Does it guarantee that I am a good driver?

Culture comes with understanding

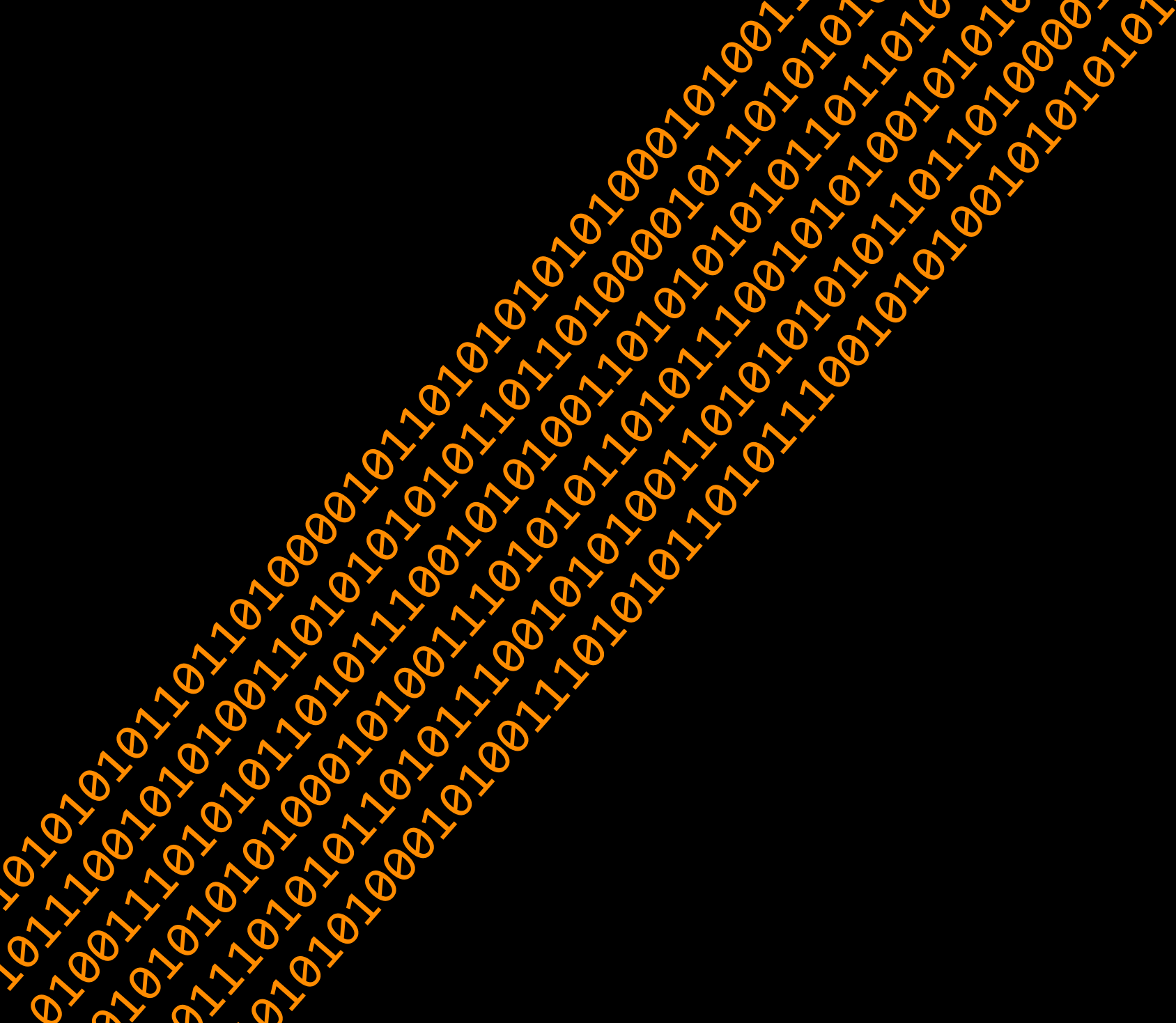
Did you know that one of the main reasons for information loss are...

UNEDUCATED
EMPLOYEES

THE TOP CAUSE OF
ORGANIZATIONAL
DATA BREACHES:

"NEGLIGENT INSIDERS"

TODAY'S ORGANIZATIONS
EXPERIENCE AN AVERAGE OF
14.4 INCIDENTS/YEAR
OF UNINTENTIONAL DATA LOSS
THROUGH EMPLOYEE NEGLIGENCE



10 Deadly Sins

Sin 10: Misunderstanding Passwords

Will you share your passwords with others?

We do this every day!

How do services store passwords?

Passwords are often similar to your other passwords

- ⌚ At least one of them can be easily accessed by the administrator of the service

Be prepared for password loss and service recovery

Sin 9: Old protocols or their default settings

Key learning points:

- ✓ SNMPv3 addresses: user-based system for access control, a means to properly authenticate users, and a method for encrypting SNMP traffic between agent and host
- ✓ SQL issues – TDS provides by default lack of encryption
- ✓ ODBC Driver – check if it has a secure networking layer built into it

NTLMv1 / NTLMv2

- ✓ Security Options in GPO allow to monitor where NTLM is used
- ✓ General direction is to get rid of NTLM

SSL / TLS

- ✓ TLS v1.3 is still an Internet Draft
- ✓ SSL 2.0 and 3.0 have been deprecated by the IETF (in 2011 and 2015)
- ✓ Disable SSL 2.0 and 3.0, leaving only TLS protocols enabled



Sin 8: Lack of SMB Signing (or alternative)

Key learning points:

- ✓ Set SPNs for services to avoid NTLM:
SetSPN -L <your service account for AGPM/SQL/Exch/Custom>
SetSPN -A Servicename/FQDN of hostname/FQDN of domain domain\serviceaccount
- ✓ Reconsider using Kerberos authentication all over
<https://technet.microsoft.com/en-us/library/jj865668.aspx>
- ✓ Require SPN target name validation
Microsoft network server: Server SPN target name validation level
- ✓ Reconsider turning on SMB Signing
- ✓ Reconsider port filtering
- ✓ Reconsider code execution prevention but do not forget that this attack leverages administrative accounts



Sin 7: No network segmentation

Key learning points:

- ✓ Network segmentation can be a blessing or a curse
 - ✓ Greater control over who has access to what
 - ✓ Allows to set rules to limit traffic between each distinct subnet
 - ✓ Allows to reduce exposure to security incidents
 - ✓ Performance: allows to reduce Broadcast Domains so that broadcasts do not spread on the entire network
-
- x VLANs limit – only 4094 different VLANs for the same network
 - x Security limits – geo locations vs. ATM clouds
 - x Managerial overhead

No-brainer or unseen network security threat?



Sin 6: Falling for (hipster) tools with issues

Key learning points:

- ✓ Worldwide spending on information security is expected to reach **\$90 billion in 2017**, an increase of **7.6 percent over 2016**, and to top \$113 billion by 2020, according to advisory firm Gartner
- ✓ With increasing budget the risk of possessing hipster tools increases too – do we know where these tools come from and what are their security practices?
- ✓ Lots of solutions where not created according to the good security practices (backup software running as Domain Admin etc.)
- ✓ Each app running in the user's context **has access to secrets** of other apps – Data Protection API
- ✓ Case of CCleaner



Sin 5: Lack of proactive approach in security

⌵ Important skills:

- ⌵ Using Windows Built-in monitoring tools
- ⌵ ETW and EVT
- ⌵ 3rd party monitoring tools

⌵ Why that matters?

- ⌵ In case of emergency situation: allows to act reasonably and based on collected data
- ⌵ Increases chances that evidence can be gathered properly
- ⌵ Pre-incident steps: use Sysmon for better knowledge about processes and network



Sin 4: Lack of forensics skills

⌚ Important skills:

- ⌚ Performing Disk Forensics
- ⌚ Memory Analysis

⌚ Why that matters?

- ⌚ Make sure all tracing features on the drive and in the system are enabled: USN, Prefetch etc.
- ⌚ Image first then play
- ⌚ Create Incident Response Procedure (most of the Customers we start the adventure with do not have it...)



Photo: the New York Times Magazine

Sin 3: Allowing unusual code execution

Key learning points:

Common file formats containing malware are:

- ✓ .exe (Executables, GUI, CUI, and all variants like SCR, CPL etc)
- ✓ .dll (Dynamic Link Libraries)
- ✓ .vbs (Script files like JS, JSE, VBS, VBE, PS1, PS2, CHM, BAT, COM, CMD etc)
- ✓ .docm, .xlsm etc. (Office Macro files)
- ✓ .other (LNK, PDF, PIF, etc.)

If **SafeDllSearchMode** is enabled, the search order is as follows:

1. The directory from which the application loaded
2. The system directory
3. The 16-bit system directory
4. The Windows directory
5. **The current directory**
6. The directories that are listed in the PATH environment variable



Sin 2: Trusting solutions without knowing how to break them

Key learning points:

- ✓ The best operators won't use a component until they know how it breaks.
- ✓ Almost each solution has some 'backdoor weakness'
- ✓ Some antivirus solutions can be stopped by SDDL modification for their services
- ✓ Configuration can be monitored by Desired State Configuration (DSC)
- ✓ DSC if not configured properly will not be able to spot internal service configuration changes

Example: how to I get to the password management portal?



According to the industry's statistics, by 2019 the
market will need 6 mln security professionals.
But only 4 to 5 million of them will have the needed
qualifications.



Sin 1: Lack of Documentation or Training

Sin 1: Lack of Documentation or Training

⌵ **Is this really the admin's sin?**

⌵ The negative side of this sin is that you need to trust people

⌵ Most companies are not prepared for the IT Staff going on a...
vacation

⌵ Set up the rules before creating the solutions

Summary: 10 deadly sins

Infrastructure can be a silent killer

Isolate infrastructure components so that in case of attack they prevent spreading

Engage with the network security guys

Review servers' and workstations' configuration periodically

Vulnerability Management

Put on the Hacker's Shoes

External + Internal + Web Penetration tests

Configuration reviews

Prevention

Start implementing the monitoring and execution prevention



10 Deadly Sins of Administrators about Windows Security



Paula Januszkiewicz

CQURE: CEO, Penetration Tester; Cybersecurity Expert

CQURE Academy: Trainer

Microsoft Regional Director

MVP: Enterprise Security, MCT

www.cquireacademy.com

paula@cquire.us



@paulacquire
@CQUREAcademy