SerNet

Wenn es wirklich zählt:

besseres Schwachstellen-Management in fünf Minuten

25. Februar 2021

Alexander Koderman

SerNet GmbH, Göttingen - Berlin

SerNet GmbH

SerNet

- gegründet 1996
- Büros in Göttingen und Berlin
- Schwerpunkt Informationssicherheit und Datenschutz
- bevorzugter Einsatz von Open Source Software
- Fachabteilungen:
  - ITSEC: technische Sicherheitslösungen für Industrie und öffentl. Hand (Firewalls, VPN und mehr)
  - verinice.: Open Source Tool für Informations-Sicherheits-Management
  - Samba: Open Source Alternative zu Windows-Servern
  - winwerk: Infrastruktur auf Basis von Microsoft-Lösungen
- SerNet ist klassischer Mittelstand, kein Risiko-Kapital, keine Bank-Kredite
- über 2500 Bestandskunden in DE, EU, US und weltweit

Alexander Koderman

SerNet

- gegründet 1977
- Homeoffice in Berlin
- Schwerpunkt Informationssicherheit und Geheimschutz
- bevorzugter Einsatz von Open Source Software
- Profil:
  - CISA, PMP, ISO 27001 LA
  - Zertifizierter BSI IT-Grundschutz Auditor a.D.
  - Consulting und Audits in Organisationen von 20 – 200.000 Mitarbeitern (seit 2004)
  - Chief Security Officer Airbus Secure Land Communications (2016-2018)
  - Teamleiter IT-Sicherheit DKB AG (2018-2019)
  - Urvater von verinice
- Alexander ist klassischer Mittelstand, kein Risiko-Kapital, ein Immobilienkredit

CVE?

SerNet

The New York Times

Digital Privacy | How to Read Privacy Labels | How to Protect Your Digital Life | 10 Simple Tips | How Apps Collect Your

Equifax to Pay at Least $650 Million in Largest-Ever Data Breach Settlement

160

18.000 neue Schwachstellen in 2020

SerNet

The New York Times

Digital Privacy | How to Read Privacy Labels | How to Protect Your Digital Life | 10 Simple Tips | How Apps Collect Your

Equifax to Pay at Least $650 Million in Largest-Ever Data Breach Settlement

160

It's an all Equifax breach / Apache Struts / CVE-2017-5638 vulnerability issue of Open Source Insight this week as we examine how an unpatched open source flaw and an apparent lack of diligence exposed sensitive data for over 140 million US consumers. We discuss what happened, how to check whether you've been affected by the breach, and whether you should replace Struts with another framework.

Synopsys has been blogging on CVE-2017-5638 since its initial disclosure in March 2017, including recommendations for how to protect yourself from the vulnerability. Read these articles for more information, and subscribe for the latest security news:

- Attacks on CVE-2017-5638 critical vulnerability escalating
- The Apache Struts vulnerability explained
- Pandora's Box–Exploits show package manager blind spots

NotPetya, Wannacry...

SerNet

WIRED BACKCHANNEL BUSINESS CULTURE GEAR MORE SIGN IN SUBSCRIBE

MIKE MCQUADE

ANDY GREENBERG EXCERPT SECURITY 08.22.2018 05:00 AM

The Untold Story of NotPetya, the Most Devastating Cyberattack in History

Crippled ports. Paralyzed corporations. Frozen government agencies. How a single piece of code crashed the world.

NotPetya, Wannacry...

SerNet

WIRED BACKCHANNEL BUSINESS CULTURE GEAR MORE SIGN IN SUBSCRIBE

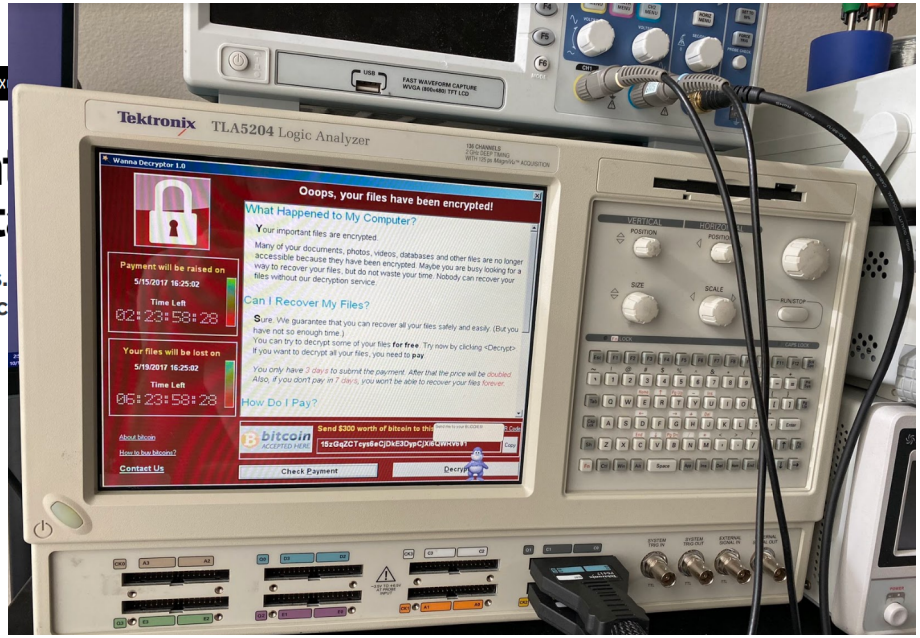
00 6E 00 2E 00 65 00 78 00 79 65 00

MIKE MCQUADE

ANDY GREENBERG

The Unt
Devast

Crippled ports.
piece of code c



NotPetya, Wannacry...

SerNet

WIRED BACKCHANNEL BUSINESS CULTURE GEAR MORE SIGN IN SUBSCRIBE

00 6E 00 2E 00 65 00 78 00 79 65 00

MIKE MCQUADE

ANDY GREENBERG EX

The Un
Devast

Crippled ports.
piece of code c

CVE-2017-0144

Newsworthy

CVSSv2 9.3 CRITICAL

CVSSv3 8.1 MEDIUM

Vulnerability Details

- **Published:** 2017-03-17
- **Modified:** 2018-06-21
- **Summary:** The SMBv1 server in Microsoft Windows Vista SP2; Windows Server 2008 SP2 and R2 SP1; Windows 7 SP1; Windows 8.1; Windows Server 2012 Gold and R2; Windows RT 8.1; and Windows 10 Gold, 1511, and 1607; and Windows Server 2016 allows remote attackers to execute arbitrary code via crafted packets, aka "Windows SMB Remote Code Execution Vulnerability." This vulnerability is different from those described in CVE-2017-0143, CVE-2017-0145, CVE-2017-0146, and CVE-2017-0148.
- **Weakness:** CWE-20
- **References:**

The Cost of NotPetya

In 2017, the malware NotPetya spread from the servers of an unassuming Ukrainian software firm to some of the largest businesses worldwide, paralyzing their operations. Here's a list of the approximate damages reported by some of the worm's biggest victims.

$870,000,000

Pharmaceutical company Merck

$400,000,000

Delivery company FedEx (through European subsidiary TNT Express)

$384,000,000

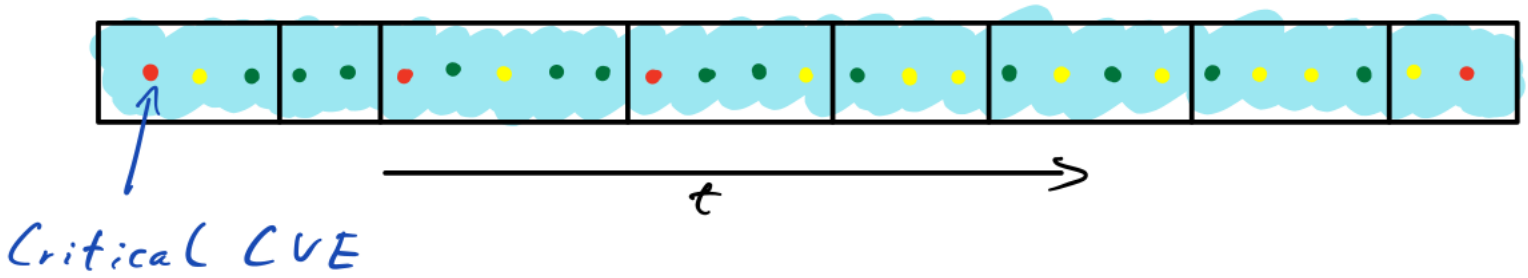
French construction company Saint-Gobain

$300,000,000

Danish shipping company Maersk

$188,000,000

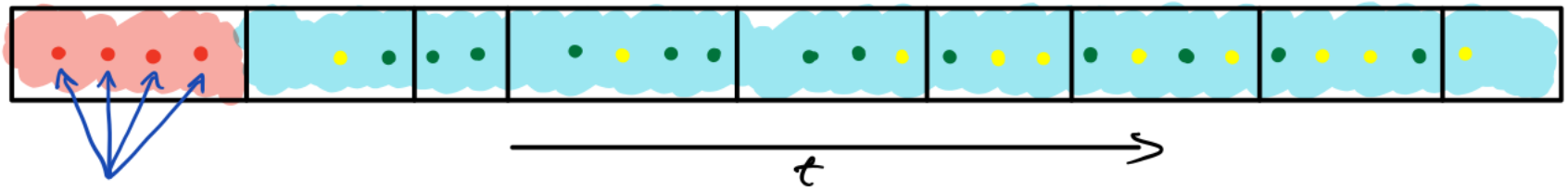
Snack company Mondelēz (parent company of Nabisco and Cadbury)



MTtP: Mean-Time-to-Patch (sollte kürzer sein als Maintenance Cycle)

Patch, Workaround, Shutdown, SIEM...

SerNet



- Patches
- Workarounds
- Shut Downs

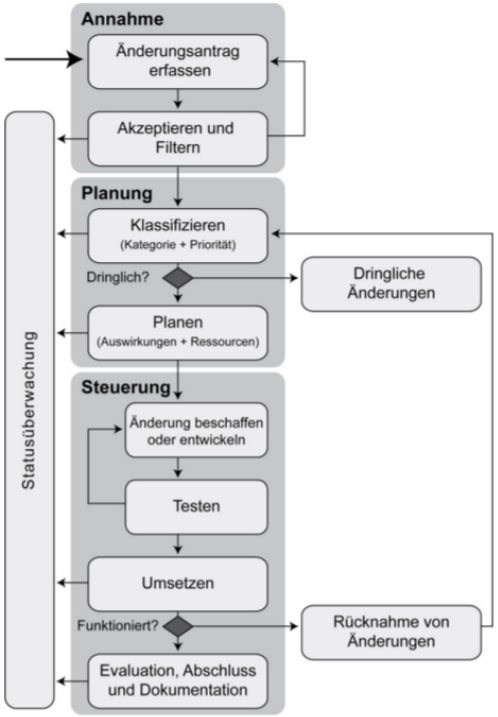
Grundschutz Kompendium

SerNet

OPS.1.1.3.M4 Planung des Änderungsmanagementprozesses [Änderungsmanager]

Jede Institution sollte für das Änderungsmanagement einen klar definierten Prozess einrichten und die Zuständigkeiten für die verschiedenen Aufgaben regeln (siehe OPS.1.1.3.M2 *Festlegung der Verantwortlichkeiten*). Alle Änderungen von Hard- und Softwareständen sowie Konfigurationen sollten über den Prozess des Patch- und Änderungsmanagements gesteuert und kontrolliert werden. Um alle Änderungen erfassen und bewerten zu können, sollten alle vom Änderungsmanagement betreuten IT-Systeme dem Änderungsmanager unterstellt sein. Änderungen an Konfiguration und Zustand der Systeme sollten damit nur noch über das Änderungsmanagement möglich sein.

Der Änderungsmanagementprozess kann, angelehnt an die IT Infrastructure Library (ITIL), wie folgt schematisch dargestellt werden:



Quelle: https://www.canada.ca/en/government/system/digital-government/online-security-privacy/patch-management-guidance.html

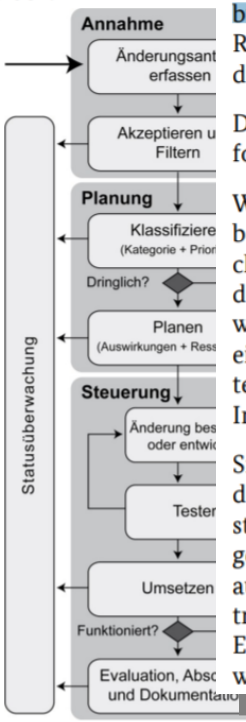
Grundschutz Kompendium

SerNet

OPS.1.1.3.M4 Planung des Änderungsmanagementprozesses [Änderungsmanager]

Jede Institution sollte für das Änderungsmanagement einen klar definierten Prozess einrichten und die Zuständigkeiten für die verschiedenen Aufgaben regeln (siehe OPS.1.1.3.M2 *Festlegung der Verantwortlichkeiten*). Alle Änderungen von Hard- und Sof
Prozess des Patch- und Änderungsmanagements
gen erfassen und bewerten zu können, sollten a
dem Änderungsmanager unterstellt sein. Änderu
ten damit nur noch über das Änderungsmanage

Der Änderungsmanagementprozess kann, ange
schematisch dargestellt werden:



SYS.1.1.M7 Updates und Patches für Firmware, Betriebssystem und Anwendungen

Häufig werden Fehler in Produkten bekannt, die dazu führen können, dass die Informationssicherheit des Informationsverbundes, wo diese betrieben werden, beeinträchtigt wird. Entsprechende Fehler können Hardware, Firmware, Betriebssysteme und Anwendungen betreffen. Diese Schwachstellen müssen so schnell wie möglich behoben werden, damit sie nicht durch interne oder externe Angreifer ausgenutzt werden können. Dies ist ganz besonders wichtig, wenn die betreffenden Systeme mit dem Internet verbunden sind. Die Hersteller von Betriebssystem- oder Software-Komponenten veröffentlichen in der Regel Patches oder Updates, die auf dem jeweiligen IT-System installiert werden müssen, um den oder die Fehler zu beheben.

Die Systemadministratoren sollten sich daher regelmäßig über bekannt gewordene Schwachstellen informieren.

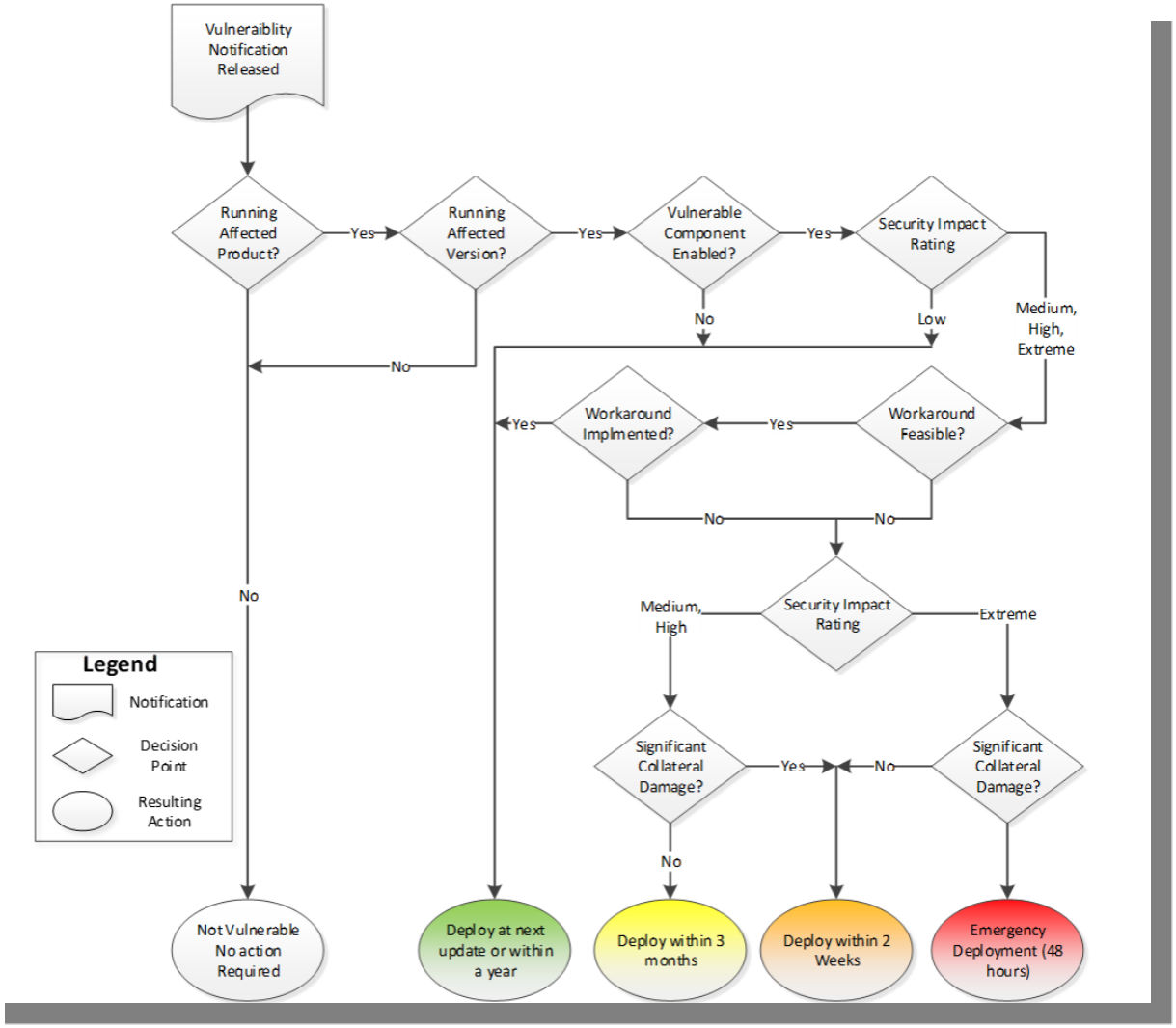
Wichtig ist, dass Patches und Updates, wie jede andere Software, nur aus vertrauenswürdigen Quellen bezogen werden dürfen. Für jedes eingesetzte System oder Softwareprodukt muss bekannt sein, wo Sicherheitsupdates und Patches erhältlich sind. Außerdem ist es wichtig, dass Integrität und Authentizität der bereits installierten Produkte oder der einzuspielenden Sicherheitsupdates und Patches überprüft werden (siehe Abschnitt "Sicherstellung der Integrität und Authentizität von Softwarepaketen"), bevor ein Update oder Patch installiert wird. Vor der Installation sollten sie außerdem mit Hilfe eines Computer-Virenschutzprogramms geprüft werden. Dies sollte auch bei solchen Paketen gemacht werden, deren Integrität und Authentizität verifiziert wurde.

Sicherheitsupdates oder Patches dürfen jedoch nicht voreilig eingespielt werden, sondern müssen vor dem Einspielen getestet werden. Für diese Tests sollten stets aktuelle, auf die Systemumgebung abgestimmte Testpläne oder automatisierte Tests genutzt werden, um ein einheitliches, aussagekräftiges Ergebnis zu erzielen. Falls sich ein Konflikt mit anderen kritischen Komponenten oder Programmen herausstellt, kann ein solches Update sonst zu einem Ausfall des Systems führen. Nötigenfalls muss ein betroffenes System so lange durch andere Maßnahmen geschützt werden, bis die Tests abgeschlossen sind. Es sollte gewährleistet werden, dass Updates, die durch automatische Update-Mechanismen eingespielt werden, ebenfalls getestet werden.

Quelle: https://www.canada.ca/en/government/system/digital-government/online-security-privacy/patch-management-guidance.html

Patchmanagement Workflow

SerNet



Quelle: https://www.canada.ca/en/government/system/digital-government/online-security-privacy/patch-management-guidance.html

Ziel

SerNet

- Monitoring von CVEs
- Monitoring von Nachrichten
- Zuordnung zu eigener Hardware & Software
- Warnung bei Exploits
- Auch ohne Scanner

http://CSTOOL.io

Try it out!

http://CSTOOL.io

Voucher Code (Sign Up → Preferences)

CSTOOL.io PRO kostenlos für ein Jahr - einlösbar bis zum 12.03.2021:

VERINICEXP

Kontakt

SerNet

Alexander Koderman, AK@sernet.de

SerNet GmbH

Bahnhofsallee 1b
37081 Göttingen

Torstraße 6
10119 Berlin

tel +49 551 370000-0
fax +49 551 370000-9

+49 30 5 779 779 0
+49 30 5 779 779 9

http://www.sernet.de