Thomas Todt

Sales Engineer EMEA & APAC

Secunia

ttodt@secunia.com

Keynote CMUG Zürich 02/2015

Secunia

Vorreiter im Bereich "Vulnerability Intelligence" und "Patch Management"

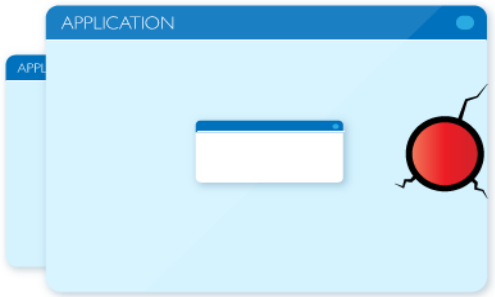
Schwachstellen Management - Folgen und die Beseitigung von Schwachstellen mittels Secunia CSI und Microsoft System Center Configuration Manager

Secunia Stay Secure

BCD SINTRAG Ein Unternehmen der ADN® Gruppe value add distribution

Configuration Manager

Softwareschwachstellen



Eine Schwachstelle, viele Überträger:

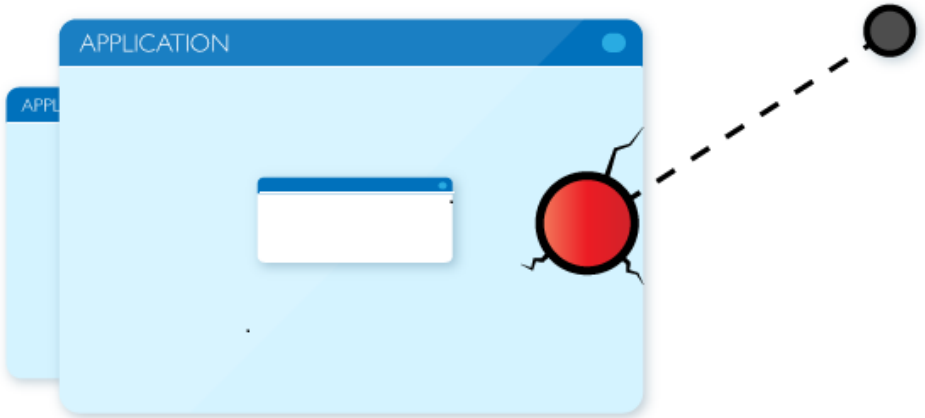
- Remote Netzwerk
- Lokales Netzwerk
- Lokales System

- Fehler im Anwendungscode:
  - Sicherheitsrisiken
  - Funktionalität

- Wo befinden sich Anwendungen?
  - Server
  - PCs, Laptops, VMs
  - Mobile Endgeräte
  - Drucker, Switches, Router
  - Maschinen und Haushaltsgeräte
  - OT Umgebungen
    - Operational Technology
      - Produktionsanlagen
      - Energieerzeugung
      - Automaten…

Von der Schwachstelle zum Exploit

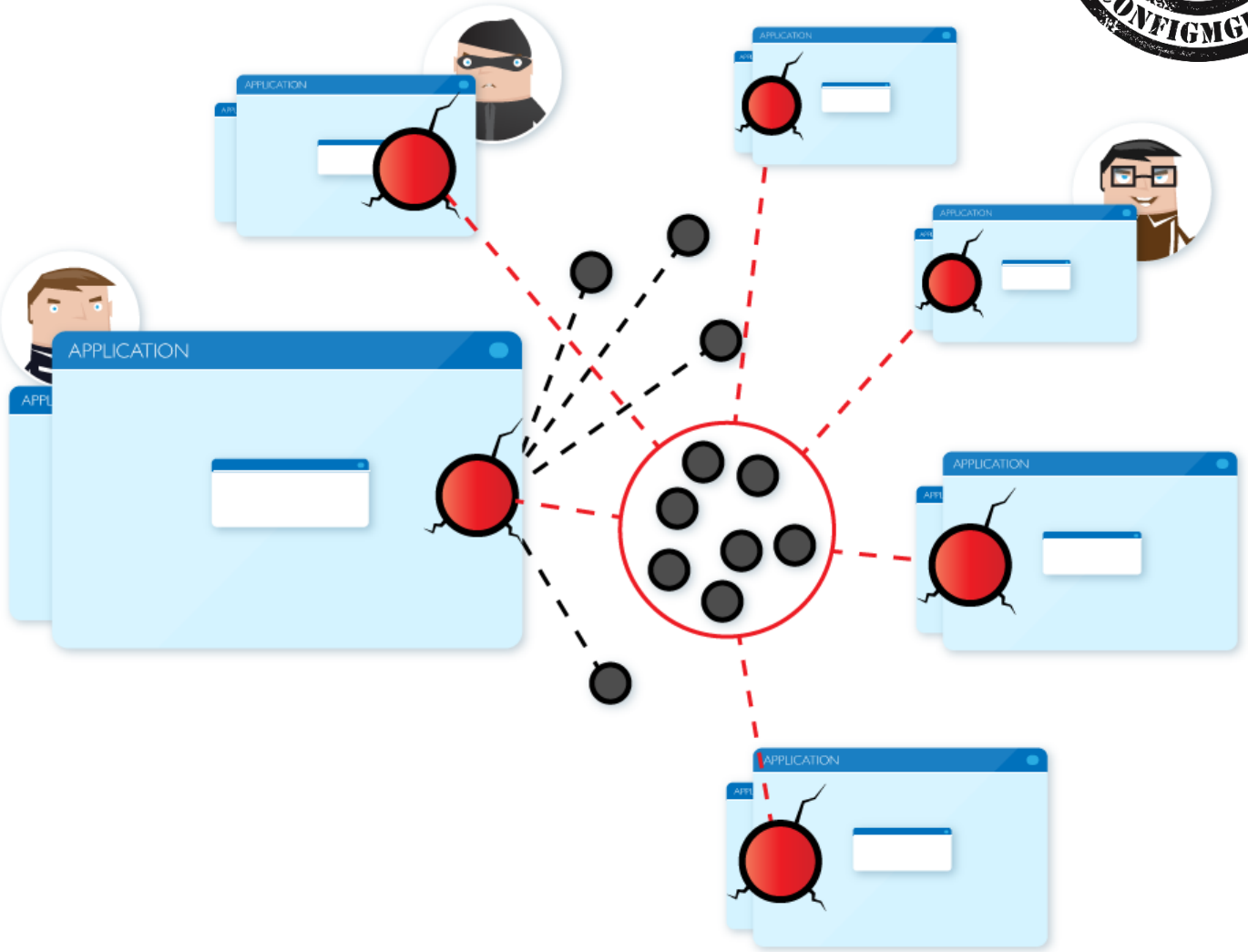
wie es zu Exploits kommt…



- Ein Hacker identifiziert eine Schwachstelle
- Er entwickelt ein Hilfsmittel, um die Schwachstelle zur Manipulation einer Anwendung auszunutzen ☛ Exploit
- Der Exploit ist erfolgreich
- Sie sind verwundbar!

Vervielfachte Bedrohungen

Das große Ganze



- Exploits werden oft im Paket verkauft:
  - Ein Paket = mehrere Exploits, die auf verschiedene Schwachstellen in unterschiedlichen Produkten abzielen
- Die steigende Anzahl von Applikationen und Geräten lässt die Anfälligkeiten und somit auch die Gefahren exponentiell anwachsen

Folgen ?

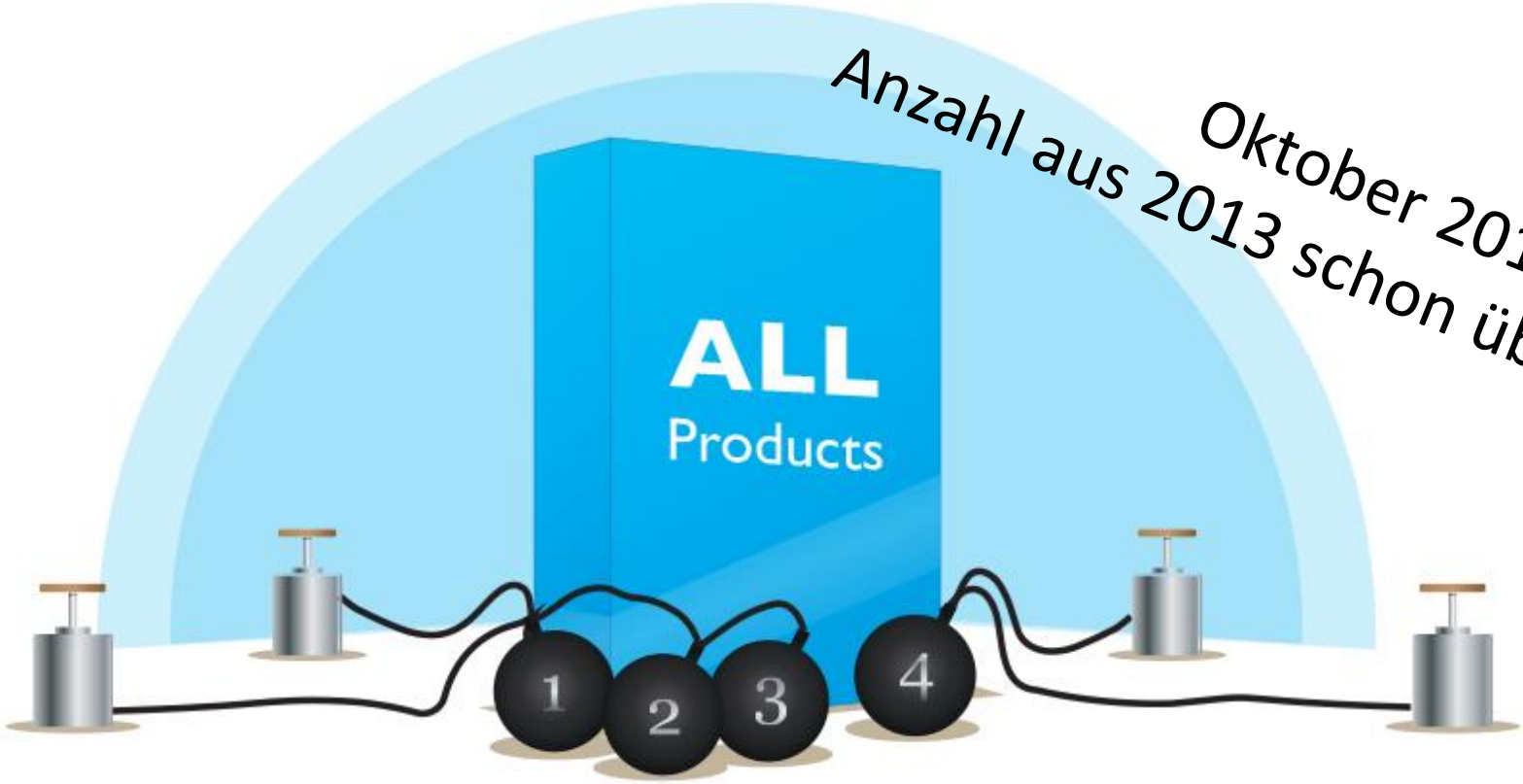
95 % aller bekannten Data Breaches werden durch längst bekannte Schwachstellen verursacht !

Schwachstellenmanagement und Risiko

- Wissen über Schwachstellen und Bedrohungen
  - Nicht alle Schwachstellen bedeuten das gleiche Risiko
- Wissen über den eigenen Bestand
  - Nicht alle Assets haben oder brauchen den gleichen Sicherheitsstandard

Schwachstellen in allen Produkten (2013)

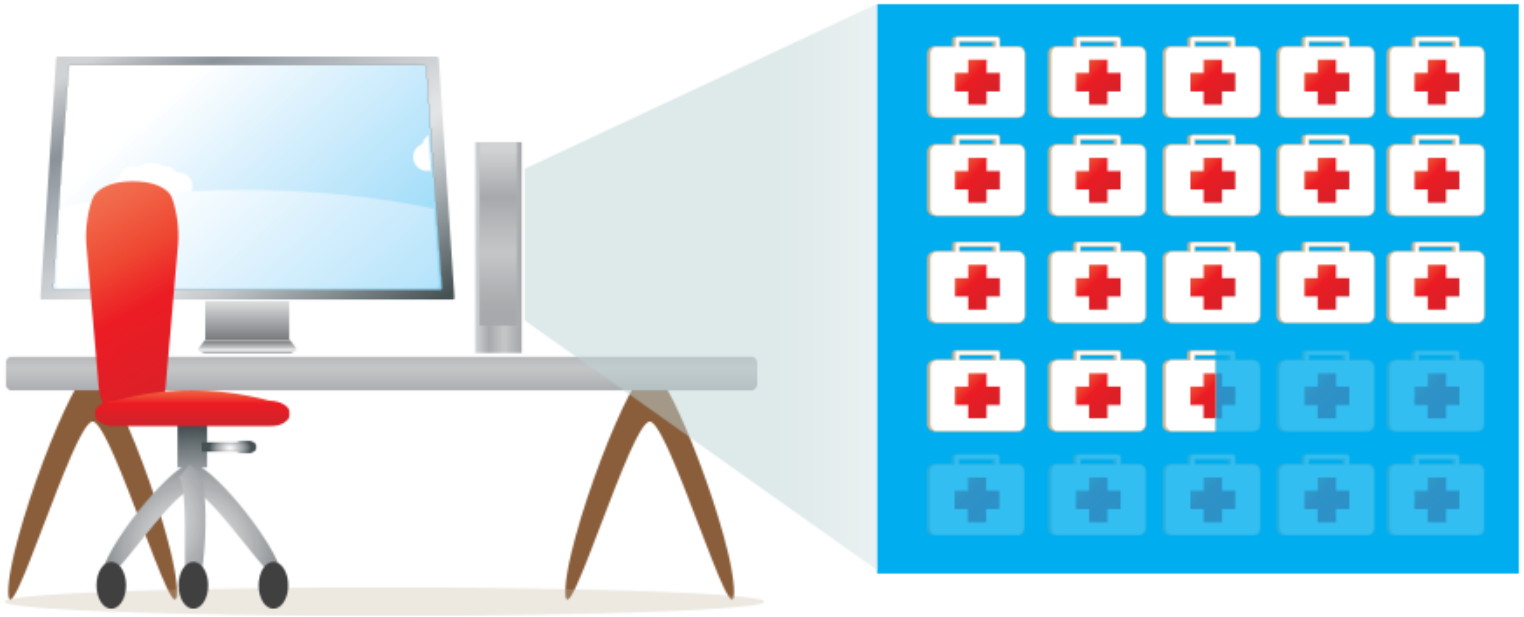
Ein Anstieg um 45% im 5 Jahrestrend



Oktober 2014:
Anzahl aus 2013 schon überschritten...

13.073 Schwachstellen in 2.289 angreifbaren Produkten

Time to Patch: Alle Produkte…

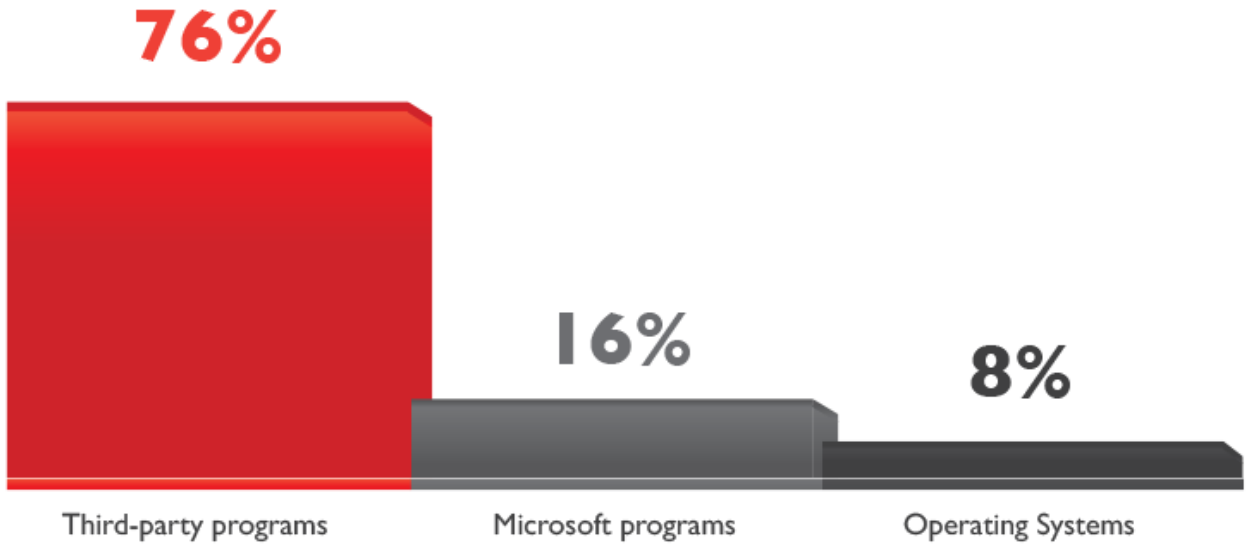


2013 gab es für 79 % der Schwachstellen schon am Tag, an dem sie entdeckt wurden einen Patch.

Das bedeutet: Es ist möglich, den **Großteil der Schwachstellen sofort zu schließen**.
Für Organisationen und User gibt es also eine Lösung für Schwachstellen in Software,
die Hauptursache von Sicherheitsproblemen.

Source: "Secunia Vulnerability Review 2014." https://secunia.com/vulnerability-review/

Darum ist es wichtige 3rd Party Programme zu Patchen



76% of vulnerabilities in 2013 affected third-party programs, outnumbering the 8% of vulnerabilities found in operating systems or the 16% of vulnerabilities discovered in Microsoft programs.

Third-party programs, rather than programs from Microsoft, are responsible for the majority of vulnerabilities in Top 50.

Source: "Secunia Vulnerability Review 2014." https://secunia.com/vulnerability-review/

Firmenüberblick

Secunia
Stay Secure

THE Open GROUP
Making standards work®

EDUCAUSE

FIRST
Improving Security Together

FINANCIAL SERVICES ISAC

ISF Information Security Forum

Gegründet: 2002

HQ: Kopenhagen, Dänemark

Regionale Büros: Minneapolis, USA

Distributor in der Schweiz:
BCD Sintrag AG

Laufende Zusammenarbeit mit führenden Industrieoriganisationen

Trusted Advisor tausender Organsiationen, einschließlich CERTS and ISACs, the White House, NATO, NIST, NERC und Mitre.

Unterstützung und laufende Zusammenarbeit:

Industrieexperten anerkennen übereinstimmenend die Innovationen in den Produkten von Secunia sowie Secunias Einsatz in der Beseitigung von Schwachstellen.

Markfokussierung

Schwachstellen Intelligenz, Schwachstellen Management und Patch Management für Enterprise, SMBs und private Benutzer

Weltberühmt	*Preisgekrönt*	*Best-in-Class*
1	2	3
Vulnerability Intelligence	Vulnerability Management	Patch Management

Research Team

Eine der größten Vulnerability Intelligence Datenbanken auf dem Markt

- Datenbank enthält Schwachstellen in Software Produkten seit 2003.
- 51,000+ Programme, Applikationen und Plugins von tausenden Software Herstellern.
- Voll CVE konform, Daten sind getestet und geprüft von Secunia's Research Team
- Einzigartige Datenbank, geistiges Eigentum von Secunia

Microsoft Alliance Partner

Microsoft® System Center

Weil das patchen von 3rd Party Produkten ein Muss für die Unternehmenssicherheit ist

Secunia ist der erste Vulnerability Security Alliance Partner des Microsoft Technology Center Programms.

Unsere Lösungen integrieren sich in Microsoft System Center 2012 und Microsoft WSUS.

Secunia ist Mitglied des Microsoft System Center Alliance Programms.

Microsoft Alliance Partner

"With System Center 2012 Configuration Manager, our customers can empower employee productivity on a wide range of devices while maintaining compliance and working to protect company data."

"With Secunia CSI and System Center 2012 Configuration Manager, our joint customers can streamline patch management processes and protect both Microsoft and non-Microsoft applications from vulnerabilities."

- Andrew Conway, Director Product Marketing, Microsoft

Secunia's Lösungsportfolio

Corporate

Corporate Software Inspector (CSI)

- **Zielgerichtetes, flexibles Patch Management**
- Sichert und aktualisiert elementare Anwendungen
- Von A-Z: Vulnerability Intelligence und Scanning plus Patch Creation und Deployment
- Microsoft System Center 2012 und WSUS integration
- Scannt PCs, Apple Mac OS X, Red Hat Enterprise Linux (RHEL)

Vulnerability Intelligence Manager (VIM)

- **Taktisches Handling von Vulnerability Bedrohungen**
- Ein einfacher und kostengünstiger Weg, um Vulnerabilities vorausschauend zu begegnen
- Liefert Echtzeit Vulnerability-Alarme
- Keine Installation notwendig

Consumer

Personal Software Inspector (PSI)

- **Kostenloses Vulnerability Management Werkzeug**
- Schützt Daten vor Cyberkriminellen
- Scannt PC Software und identifiziert unsichere Programme
- Installiert automatisch Softwaresicherheitsupdates und sorgt so für einen sicheren PC
- Verfügbar in Arabisch und 7 weiteren Sprachen

PSI für Android

- **Kostenlose Version für Smartphones und Tablets**
- Scannt Apps, die von Google Play Store als auch von externen Quellen installiert wurden .
- Alarmiert Benutzer über Apps mit bekannten Vulnerabilities.
- Prüft auf schnelle Umsetzung von Sicherheitsupdates.

Secunia CSI 7 - Livedemo

Livedemo Corporate Software Inspector CSI 7:

Detect, Identify, Analyze and Patch directly from SCCM 2012 console

PATCHMANAGEMENT THE EASY WAY...

Weitere Infos

Keep up to date with our latest news and research

Facebook
facebook.com/Secunia

Twitter
twitter.com/Secunia

LinkedIn
linkedin.com/company/secunia

Secunia community
secunia.com/community/profile

Secunia papers, reports, vulnerability data, webinars…
secunia.com/resources

Digicomp Kurse neu

https://www.microsoft.com/learning/en-us/course.aspx?ID=20695A&Locale=en-us

https://www.microsoft.com/learning/en-us/course.aspx?ID=20696A&Locale=en-us

Herzlichen Dank

Thomas Todt@Secunia.com

Bewertung der Session: Configmgr.ch

- Xing: https://www.xing.com/net/cmce
- Facebook: https://www.facebook.com/groups/411231535670608/
- Linkedin: http://www.linkedin.com
- Twitter: https://twitter.com/configmgr_ch

Stay Secure!

www.secunia.com

Secunia
Mikado House, Rued Langgaards Vej 8, 4th floor
DK-2300 Copenhagen S
Denmark

Phone: +45 7020 5144
Fax: +45 7020 5145

Secunia Inc.
Lake Calhoun Business Center, Suite 420
3033 Excelsior Boulevard
Minneapolis, MN 55416
USA
Phone: +1 888 924 8265
Fax: +1 888 924 8266