T.I.S.P. TeleTrusT Information Security Professional

TeleTrusT Pioneers in IT security.

T.I.S.P. Community Meeting

Berlin, 02. - 03.11.2015

CERT-Management

Ein kleines How-To

Detlef Hauke

Footfalls Ltd.

1. Begrüßung
2. Zur eigenen Person
3. Einstieg ins Thema
    1. Eigene Lösungssuche
    2. Erfahrungen aus Kundenprojekten
    3. Evtl. doch kein leichtes Thema?

„CERT-Management? Was ist denn das?“

und …

„Brauchen wir das wirklich?“

1. Das „Warum?“
2. Notwendigkeit
    - Abhängig von der eigenen Infrastruktur
    - Closed-shop Systeme haben andere Bedrohungslage als Server in einer DMZ
    - Einfluss durch Kunden
    - BSI M 2.35 Informationsbeschaffung über Sicherheitslücken des Systems

1. Begriffsbestimmung
    1. Worum es eigentlich geht
    2. CERT = Computer Emergency Response Team
    3. Aufgaben

Aber …

Umgangssprachlich meint CERT Management
die Informationsbeschaffung und
Bearbeitung von Sicherheitslücken/-risiken

1. … was im allg. unter dem Oberbegriff CERT-Management verstanden wird

Oder …

Den Umgang und die Behandlung von

Common Vulnerabilities and Exposures (CVE)

1. … und worum es tatsächlich geht

   Common Vulnerabilities and Exposures = Industriestandard mit dem Ziel einer einheitlichen Namenskonvention für Sicherheitslücken in IT-Systemen

Das Vorgehen …

Ein Prozess des Prozesses wegen?

1. Keine Musterlösung
2. Immer an die Organisation angepasst
3. Im Zweifelsfall ist eine Liste in Excel besser als keine Dokumentation
4. Wer soll die Informationen beschaffen
5. Wer ist f.d. Bewertung verantwortlich
6. Welche Rolle spielen
    1. ITSB
    2. Sicherheitsmanagement
    3. Administratoren
    4. Kunden
7. Befindlichkeiten der Beteiligten

1. Muss es CERT-Bund o.ä. sein
2. Welchen Vorteil bringt Informationsbeschaffung beim Hersteller
3. Mailinglisten der Hersteller

Einige Links:

1. Redhat
   https://access.redhat.com/security/cve/#/
2. Ubuntu
   http://www.ubuntu.com/usn/
3. Common Vulnerabilities and Exposures (CVE®)
   http://www.cve.mitre.org/about/index.html
4. Debian
   https://lists.debian.org/debian-security-announce/
5. National Vulnerability Database
   https://nvd.nist.gov/home.cfm
6. Cisco
   http://tools.cisco.com/security/center/navigation.x?i=118

Fragen / Anmerkungen /
Eigene Erfahrungen

1. Fragerunde

email: detlef.hauke@footfalls.biz
mobil: +49 171 2134578
twitter: @detlefhauke
facebook: https://www.facebook.com/detlefhauke

Vielen Dank für Ihr Interesse!