Aktuelle Informationen zur Informationssicherheit

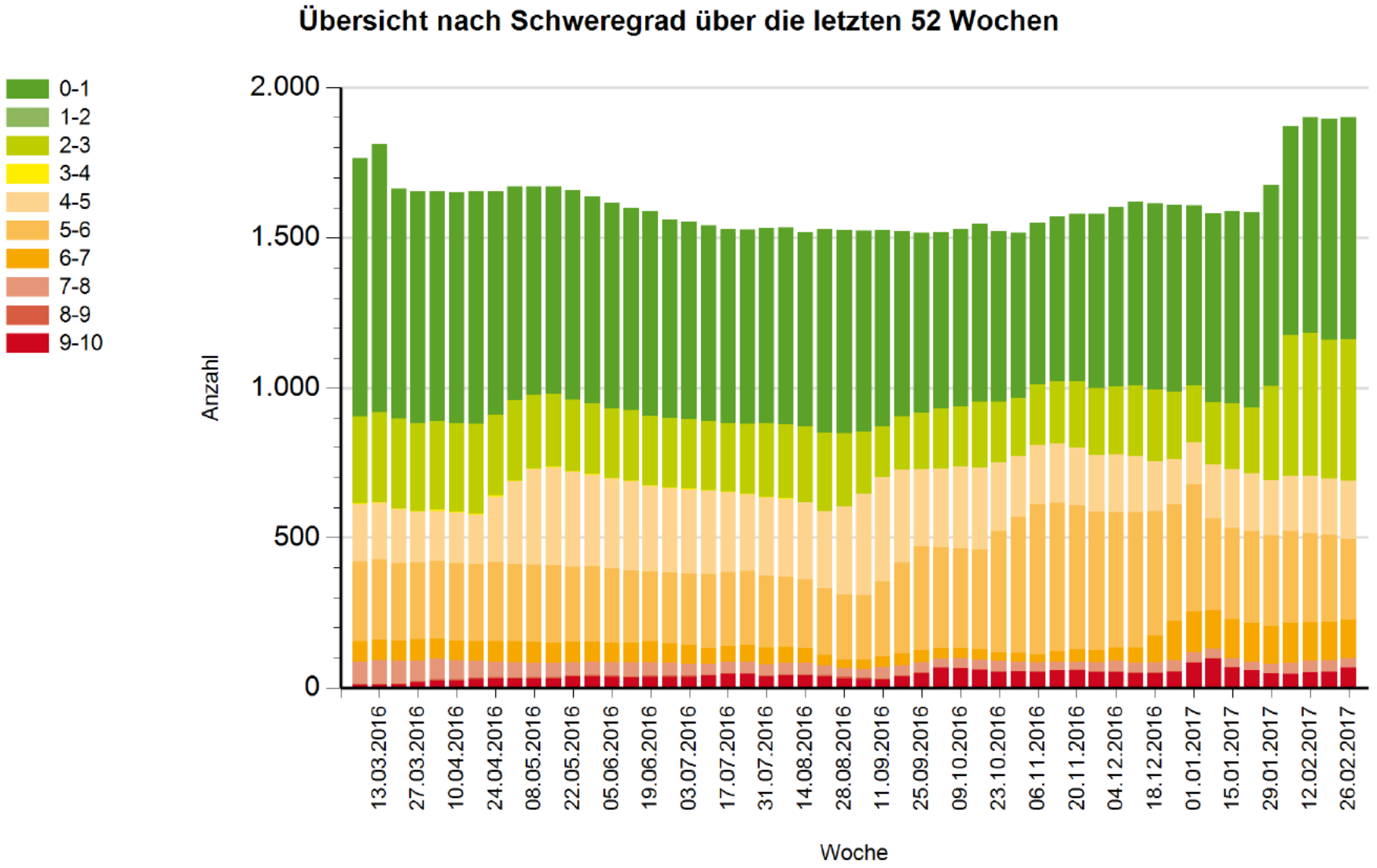
Guido Bunsen / IT Manager Security

IT Center | RWTH AACHEN UNIVERSITY

Die RWTH bekommt einen Sicherheitsprozess

- Bislang wurden einige Aspekte zur IT-Sicherheit in der Netzordnung geregelt
- In Zukunft wird es einen klar beschriebenen Sicherheitsprozess geben:
  - Sicherheitsleitlinie
    - Stellenwert der IS
    - Bekenntnis der Leitung
    - Sicherheitsziele
    - Organisationsform
  - Sicherheitsstrategie, Sicherheitskonzept

Aktuelle Zahlen zu den Greenbone-Scans



Übersicht über die häufige und kritische Schwachstellen

- General
  - 19 x 103674 OS End Of Life Detection

Web application abuses
  - 11 x 802330 PHP Multiple Vulnerabilities - Sep11 (Windows)
  - 11 x 902836 PHP com_print_typeinfo() Remote Code Execution Vulnerability (Windows)
  - 19 x 105888 PHP End Of Life Detection (Windows)
  - 20 x 807092 PHP phar_fix_filepath Function Stack Buffer Overflow Vulnerability - Mar16 (Windows)
  - 20 x 808674 PHP Multiple Vulnerabilities - 05 - Aug16 (Windows), Web application abuses
  - 23 x 808606 PHP Denial of Service And Unspecified Vulnerabilities - 01 - Jul16 (Windows)

Übersicht über die häufige und kritische Schwachstellen (2)

- Buffer overflow
  - 11 x 803317 PHP _php_stream_scandir() Buffer Overflow Vulnerability (Windows)
- Denial of Service
  - 21 x 808672 PHP type confusion Denial of Service Vulnerability (Windows)"
- Windows
  - 37 x 140151 SMBv1 Unspecified Remote Code Execution (Shadow Brokers)
- ~

Wiki zum Austausch für RWTH Admins

- Es kann gerne genutzt werden, um erfolgreiche Herangehensweisen an IT Probleme zu dokumentieren. Bitte neue Artikel nur im Namespace it_best_practise anlegen.
- Für den Austausch nicht nur zu Fragen der IT-Sicherheit
- Login per TIM-Kennung über Shibboleth/SAML
- Link:
  https://wiki.informatik.rwth-aachen.de/doku.php?id=it_best_practise

- Danke an André Stollenwerk und Frank Knoben

Vielen Dank
für Ihre Aufmerksamkeit