EUNIS 2020 Malaga

Universität Malaga

- Alle Anhänge geblockt
- POP3 und IMAP ohne Sicherungen gesperrt (Vorgeschaltet: Auswertung von Logs, Frist an User innerhalb von 5 Tagen zu reagieren)

Gaute Wangen, Uni Trondheim (NTNU)

- Digitital security section mit 8 Mitarbeitern (bei 7.500 Mitarbeitern)
- Widerspruch zwischen Akademischer Freiheit und IT-Sicherheit/Datenschutz
- Ausweisung von mehreren wissenschaftlicher Mitarbeitern(zuletzt 2 Iranern) wegen Spionage
    - Wirtschaftsspionage
    - Illegale Datensammlung(2,2 Prozent der Mitarbeiter wurden mehr als 5 Mal dafür kontaktiert)
- 151 Vorfälle seit 2017 (Mehrheit in 2019)
- Test mit (freiwilligen) Probanden, die wussten angegriffen zu werden aber sie wussten nicht wie. Angriff mit Spearfishung mit öffentlich verfügbaren Informationen (inhaltlich Neuerungen bei DSGVO, Vergütung). Mehrzahl der Probanden wurde erfolgreich angegriffen.

Administratives Department für IT-Sicherheit der Bayrischen Hochschulen

ISMS - Vorgehen

- 2017 Audits
- 2018 Policy Scope
- 2019 Organisation
- 2019/2020 Communication Awareness (Gegenwärtig schon gute Werte)
- 2020 Risiken
- 2020/2021 Reports

Ziel: 3 Mitarbeiter pro Einrichtung für IT-Sicherheit IT-Sicherheit ist kein Prozess sondern ein Kreislauf

Don Stikvoort CSIRT, Open CSIRT Foundation

- https://opencsirt.org/
- https://www.first.org/education/FIRST_PSIRT_Service_Framework_v1.0
- https://opencsirt.org/csirt-maturity/sim3-and-references/
- GFCE GCFM
- http://sim3-check.opencsirt.org/ Tool zur Selbsteinschätzung

Asbjørn Reglund Thorsen, An API for Management to check on production-readiness!

Thorste Küfer, Vulnerability management at University of Münster

automatisierte Suche nach offenen Ports in Münster OpenVAS; Freemium-Modell; Greenbone 2 Installationen für externe und interne Sicht

- wöchentlicher Scan aller Systeme, die vom Internet erreichbar sind
- bei Bedarf interne Scan (insb. bei Sicherheitswarnungen, zB RDP)
- Seltene falsch-positive Ergebnisse

kommerzielle Version: Einrichtung etwa 40 TEUR, Betrieb 5 TEUR jährlich DFN will SOC einführen

Asbjørn Reglund Thorsen, Physical access. Live hacking

Demonstration vermeintlich harmloser USB-Sticks, die als Keylogger arbeiten, Befehle ausführen oder Daten abziehen können. Bad USB: Stick speichert Energie um auf einen Schlag soviel Energie zurückzuspeisen, dass das Gerät kaputtgeht

Diskussion

- TLS 1.2
- Emails nicht mittels (Allen) Antworten-Funktion für andere Kontexte nachverwenden, um Gewöhnungseffekte zu vermeiden
- Online-Test für Schadcode: https://uni-muenster.de/ZIVtest/vt-demo/ mit Anmeldung auch Cuckoo, BSI MISP