HOCHSCHULE ANHALT University of Applied Sciences

ADMIN-GUIDE BEI SCHWERWIEGENDEN IT-VORFÄLLEN

Ruhe bewahren & IT-Vorfall melden

Lage analysieren, Beweise sichern ohne Systeme zu verändern!

HSA-IT-Vorfallnotrufnummer: +49 (0) 3496 67 5500

Analyse:

- Systeme welcher Art sind betroffen?
- Wie viele Systeme sind seit wann betroffen?
- Welcher Nutzerkreis / (Fach-) Bereich ist betroffen?

Aktionen:

- Netztrennung der betroffenen Systeme (LAN und WLAN)
- Betroffene Systeme eingeschaltet lassen
- **Sicherung der betr. Systeme gegen Zugriff und Veränderung**
- Kennzeichnung der betroffenen Systeme (z. B. Aufkleber)
- Betroffene Nutzer informieren, befragen und beruhigen
- Suche nach IOCs* auf anderen evtl. betroffenen Systemen, Test anderer Systeme unter Verwendung des „security incident survey cheat sheet for server adminstrators“ (siehe Rückseite)
- Sicherung von Logdateien, Systemprotokollen und Beweisen
- Überprüfung der Backups auf Betroffenheit & Verfügbarkeit
- Erstellung forensischer Abbilder der betroffenen Systeme**

! Achtung:

- Betroffene Systeme nicht verändern! Kein blinder Aktionismus!
- Keine Anmeldung auf sauberen Systemen mit privilegierten Accounts!
- Keine Informationen an die Öffentlichkeit! Alles dokumentieren!
- Zuständigkeiten einhalten! Weitere Anweisungen abwarten!

*Indicators Of Compromise (Datei-Hashes, E-Mail-Header, Anmeldeversuche, IP-Adressen, ungewöhnliche Befehlseingaben von Nutzern, ungewöhnliche oder mit falschem Nutzer laufende Prozesse mit hoher Rechenzeit, unberechtigt geöffnete Ports, Registry-Einträge)

**ISC_VA_F04_01_R01-09_ErstellenForensischesAbbild.docx