Handreichung zur IT-Sicherheit

Informationen und Empfehlungen zum Schutz vor Schadsoftware (*Stand: 18.12.2019*)

Präventionsmaßnahmen

Das ZIV filtert soweit wie möglich schadhafte E-Mails aus und versucht den Zugriff auf böswillige Webseiten zu verhindern. Das WWU-CERT versucht verwundbare Server und Dienste mit den Verantwortlichen abzusichern.

Trotz dieser Maßnahmen sind die folgenden Punkte zu beachten:

1. Aktueller Softwarestand (Betriebssystem, Browser, Office, E-Mail-Programm). Siehe auch [1].
2. Aktiver Virenschutz inklusive HIPS und Exploit Prevention. Siehe auch [2].
3. Nicht dauerhaft als Administrator arbeiten. Siehe auch [3].
4. Automatische Ausführung von Office-Makros verhindern.
5. Dienstliche Daten nur auf Netzlaufwerken von ZIV und IVVen speichern. Dateisystem-Snapshots und regelmäßige Backups einrichten. Zugriffsrechte so differenziert wie möglich setzen.
6. Sensibilisierung der Nutzer. Verweis auf die IT-Sicherheits-Webseiten [4].

Vorgehen bei Schadsoftware-Befall

(Siehe auch [5])

1. Rechner so schnell wie möglich vom Netzwerk trennen. Nicht Remote und nicht als Administrator einloggen!
2. Benachrichtigungen
   a. Meldung an IV-Sicherheitsbeauftragten vor Ort (Siehe [6])
   b. Meldung an WWU-CERT (cert@uni-muenster.de)
   c. Ist von einem größeren Vorfall auszugehen, der Auswirkungen auf die gesamte WWU haben kann, Meldung mit dem Wort "Alarm" im Betreff an IVV-Admin-Mailingliste (ivv-admins@uni-muenster.de)
3. Klärung der Ursache des Vorfalls.
4. Änderung aller Passwörter des/der betroffenen Nutzer/s.
5. Weitere möglicherweise infizierte Rechner identifizieren.
6. Infizierte Rechner mit neuem Betriebssystem-Image versehen. Eine zuverlässige Bereinigung ist nicht möglich.
7. Falls nötig, jetzt Daten wiederherstellen.
8. Je nach Schwere des Vorfalls Abschlussbesprechung. Was kann verbessert werden?

---

[1] Ab 15.01.2020 können Windows 7 und Windows Server 2008 Endgeräten nur noch mit zusätzlichen Schutzmaßnahmen betrieben werden oder es muss Extended Support eingekauft werden.

[2] https://www.uni-muenster.de/imperia/md/content/iv-sicherheit/empfehlung_zum_einsatz_von_sophos_an_der_wwu.pdf

[3] https://www.uni-muenster.de/imperia/md/content/iv-sicherheit/standards_f__r_sichere_administration.pdf

[4] https://www.uni-muenster.de/IT-Sicherheit/anwender/index.html

[5] https://www.uni-muenster.de/CERT/services/incident-response.html

[6] https://www.uni-muenster.de/imperia/md/content/iv-sicherheit/intern/iv-sicherheitsbeauftragte_der_wwu.pdf