Digitaler Ersthelfer

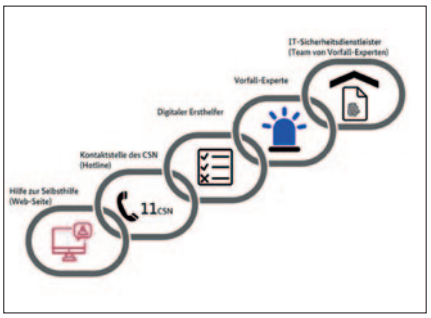
Das deutsche Bundesamt für Sicherheit in der Informationstechnik (BSI) veröffentlichte einen Leitfaden für die „Erste Hilfe“ bei IT-Zwischenfällen. Der Leitfaden bildet unter anderem die Grundlage für die Ausbildung als digitaler Ersthelfer in Unternehmen sowie für Privatpersonen.

Wir alle waren schon mit ähnlichen Vorfällen konfrontiert: Auf dem Desktop des Laptops tauchen Programme auf, die nicht von uns selbst installiert wurden. Selbst nach einer Deinstallation werden diese erneut eigenständig installiert. Oder nach einer Suchanfrage über *Google* gelangte man nicht zur gewünschten Ergebnisseite. Es öffnet sich stattdessen eine merkwürdige Seite, die die Suchergebnisse anzeigt. Oder aber der Versuch, ein Dokument zu öffnen, schlägt fehl. Es öffnet sich eine Meldung mit der Aufforderung, ein Lösegeld zu bezahlen.

Leitfaden. Das deutsche *Bundesamt für Sicherheit in der Informationstechnik (BSI)* veröffentlichte einen Leitfaden für die „Erste Hilfe“ bei derartigen IT-Zwischenfällen. Er bietet die Grundlage für die Ausbildung zum „digitalen Ersthelfer“. Der Leitfaden wird vom BSI online angeboten und endet mit einer Zertifizierung und der Eintragung in einem speziellen Netzwerk. Für die First-Level-Unterstützung sind im Cyber-Sicherheitsnetzwerk digitale Ersthelfer registriert, die schnell telefonische Ersthilfe anbieten, etwa zur Behebung von kleineren IT-Störungen- und IT-Sicherheitsvorfällen an. Dieses Netzwerk kann online sowie telefonisch in Anspruch genommen werden.

Hilfe zur Selbsthilfe. Bei diesem Leitfaden geht es nicht nur um die richtige Reaktion bei sicherheitsrelevanten Zwischenfällen, sondern generell um die erste Hilfe von Anlaufstellen, an die sich Endanwender privat oder in Betrieben wenden können. In der Hilfekette steht an erster Stelle die Hilfe zur Selbsthilfe. Auf der Website des *BSI* werden relevante Hilfestellungen angeboten *(www.bsi.bund.de)*.

Das Lernziel des Führers ist es, grundlegende Begriffsbestimmungen kennenzulernen und zu unterscheiden, die beschriebenen Fehler des jeweiligen Systems richtig zu erkennen und die richtigen Ratschläge zu geben bzw.



Digitale Rettungskette: Unterstützung für KMUs sowie Privatpersonen bei der Reaktion auf IT-Sicherheitsvorfälle durch Cyber-Angriffe.

nächsten Schritte einzuleiten. Im ersten Teil des Ratgebers werden allgemeine Probleme wie das Nicht-Hochfahren eines Systems, typische Fehlermeldungen oder Funktionsfehler von Programmen oder Drucker beschrieben. Dieser Teil wird, wie auch die nachfolgenden, durch eine genaue Zusammenfassung und einen Kurztest abgeschlossen.

Im zweiten Teil geht es um sicherheitsrelevante Fehler, für die ein typischer Anwender Hilfe suchen kann. Wieder werden Fachbegriffe erklärt, die für weitere Schritte erforderlich sind. Im inhaltlichen Bereich beschreibt die Leitlinie typische Vorfälle die sicherheitsrelevant für das einzelne System aber auch das ganze Netzwerk sein können.

Neben rein sicherheitsrelevanten technischen Störungen wie Botnetze oder Ransomware, geht das Werk auch auf die Gefahren von „Social Engineering“ ein, wie Passwortänderungsanfragen, Ausspionieren von Daten oder unbegründete Weiterleitung von Anfragen.

Vorfall-Experten. Ein wesentlicher Teil widmet sich der Problematik von Viren und Warnhinweisen. Neben dem richtigen Verhalten bei einer Warnmeldung durch einen Virenscanner, werden auch die weiteren Schritte, wie das Einbeziehen eines „Vorfall-Experten“, sowie die Verifizierung der Warnmeldung auf der Serviceseite *www.virustotal.com* beschrieben. Vorfall-Experten können Bürger sowie kleine und mittelständische Unternehmen bei der Vorfallbearbeitung unterstützten z. B. bei der Analyse von IT-Sicherheitsvorfällen (telefonisch, per Remote-Unterstützung oder vor Ort), der Eindämmung des Schadensausmaßes eines IT-Sicherheitsvorfalls, der Ermittlung der Ursachen eines IT-Sicherheitsvorfalls sowie der Wiederherstellung der Systeme nach einem IT-Sicherheitsvorfall. Dem digitalen Erst-helfer werden auch Grenzen gesetzt. Konkret wenn die zur Beseitigung erforderliche Expertise die Kompetenzen des digitalen Ersthelfers gemäß Leitfaden übersteigt. Dafür werden die erforderlichen nächsten Schritte im Detail beschrieben.

Digitale Rettungskette. In der in Deutschland bundesweit einheitlichen „Digitalen Rettungskette“ arbeiten digitale Ersthelfer, Vorfall-Experten und IT-Sicherheitsdienstleister aufeinander abgestimmt. Sie bilden ein übergreifendes Komplettsystem, das, beginnend mit der Identifizierung, über Hilfestellung, bis hin zur umfassenden Lösungsbetreuung und Vorfallklärung, eine Reihe unterschiedlicher reaktiver Hilfsangebote etabliert.

Im letzten Teil wird auf den richtigen Umgang mit den Anfragestellern und der korrekten Dokumentation eingegangen. Professionelles Verhalten am Telefon wird ebenso geschult wie konkrete Verhaltensregeln bei einem Sicherheitsvorfall. Sehr detailliert gehen die Autoren auf das Thema „Weitere Rettungskette“ ein. Also die Schritte, die zu setzen sind, wenn der digitale Ersthelfer auch nicht mehr in der Lage ist weiterzuhelfen. Interessant und für die Weiterbildung in diesem Bereich unerlässlich sind auch die weiterführenden links zu den aktuellen Phishing-Warnungen *(www.verbraucherzentrale.de/wissen/digitale-welt/phishingradar/phishingradar-aktuelle-warnungen-6059)*, zum Auslesen von E-Mail-Headern *(www.verbraucherzentrale.de/wissen/digitale-welt/phishingradar/so-lesen-sie-den-mailheader-6077)* und zum sicheren Umgang mit Passwörtern. *Bernhard Otupal*

GRAFIK: BSI