Bundesamt
für Sicherheit in der
Informationstechnik

Cyber-
Sicherheitsnetzwerk

Deutschland
Digital•Sicher•BSI•

Die „Digitale Rettungskette“ des Cyber-Sicherheitsnetzwerks

Das Cyber-Sicherheitsnetzwerk

Die fortschreitende Digitalisierung zwingt zunehmend auch kleine und mittlere Unternehmen (KMU) ihre Geschäftsabläufe zu digitalisieren, um wettbewerbsfähig zu bleiben. Damit einhergehend steigt auch das Risiko eines IT-Sicherheitsvorfalls. Während Kritische Infrastrukturen, Konzerne und große Unternehmen nach einem IT-Sicherheitsvorfall auf interne Notfallteams zurückgreifen können, stehen hingegen KMU und Bürger meist alleine da. Ohne die notwendige Expertise und Erfahrung kann es schwer werden, einen solchen Vorfall zu bewerten, die richtigen Schritte zu ergreifen und den Schaden einzudämmen.

Hier setzt das Cyber-Sicherheitsnetzwerk (CSN) des Bundesamtes für Sicherheit in der Informationstechnik (BSI) an. Mit dem CSN wird eine flächendeckende dezentrale Struktur aufgebaut, über die KMU und Bürger bei IT-Sicherheitsvorfällen effiziente Unterstützung erhalten können.

Das CSN ist ein freiwilliger Zusammenschluss von qualifizierten Experten für die Vorfallsbearbeitung, die sich bereit erklären, ihr individuelles Fachwissen zur Behebung von IT-Sicherheitsvorfällen zur Verfügung zu stellen. Sie unterstützen durch die Übernahme reaktiver Tätigkeiten, IT-Sicherheitsvorfälle zu erkennen und zu analysieren, das Schadensausmaß zu begrenzen sowie weitere Schäden abzuwenden. Dabei kann die Unterstützung je nach Vorfall und Zielgruppe unterschiedlich ausfallen. Das Netzwerk zeichnet sich durch einen kooperativen Ansatz, von der gezielten Qualifizierung bis hin zum Erfahrungsaustausch, aus.

Das BSI betreibt die Kontaktstelle (Hotline) und stellt für die einzelnen Eskalationsstufen den entsprechenden Rahmen sicher, angefangen bei den Anforderungen der jeweiligen fachlichen Qualifikation, über die Zertifizierung von Vorfall-Experten und IT-Dienstleistern bis hin zur Registrierung von Teilnehmern.

Die Digitale Rettungskette

Um für jeden Betroffenen die passende Unterstützungsleistung anbieten zu können, sieht das CSN eine sogenannte Digitale Rettungskette vor, die aus mehreren Eskalationsstufen besteht. Sie erlaubt es Betroffenen, mit ihren IT-Sicherheitsvorfällen an einem beliebigen Glied einzusteigen, aber auch aktiv an das nächste Glied in der Kette zu eskalieren, sollte die momentane Stufe nicht in der Lage sein, den Vorfall zu beheben. Dabei reicht die Unterstützung in den Stufen der Digitalen Rettungskette von schriftlichen Leitfäden über eine telefonische Unterstützung durch die Experten des Netzwerkes bis hin zu einem Team von Experten, das vor Ort tätig werden kann.

Hilfe zur Selbsthilfe

An erster Stelle der Digitalen Rettungskette steht die Hilfe zur Selbsthilfe. Hierzu finden die Betroffenen auf der Webseite des CSN Informationen zu Erste-Hilfe-Maßnahmen, die sie bestenfalls direkt auf ihr Problem anwenden können. Diese Maßnahmen setzen sich zusammen aus drei Bausteinen: Informationen / Leitfäden und damit einhergehend weiterführende Links, einer anonymen Meldestelle sowie einem Selbsteinschätzungstest. Dieser liefert Betroffenen eine erste Einschätzung, welche der Eskalationsstufen in der Digitalen Rettungskette kontaktiert werden sollte. Für die Kontaktaufnahme stehen Betroffenen die Kontaktdaten der Experten des CSN auf den Webseiten zur Verfügung.

Kontaktstelle des CSN (Hotline)

Betroffene eines IT-Vorfalls entscheiden selber, ob sie zunächst eigenständig die Erste-Hilfe-Maßnahmen über die Webseite in Anspruch nehmen, direkt einen Experten kontaktieren oder sich an die Kontaktstelle des CSN (Hotline) wenden. Diese ist über eine kostenfreie Telefonnummer 0800-274 1000 zu erreichen und hilft Betroffenen, ohne direkt zum jeweiligen Vorfall zu beraten, den IT-Sicherheitsvorfall einzuschätzen sowie bei der Entscheidung, welches Glied der Digitalen Rettungskette (Eskalationsstufe) sie kontaktieren sollten. Am Ende eines Gespräches erhalten die Betroffenen eine Liste von Experten der gewählten Eskalationsstufe, mit denen sie selbstständig in Kontakt treten und eine Vorfall-Beseitigung beauftragen können. Die Kontaktaufnahme mit Experten beruht auf freiwilliger Basis und es steht allen Betroffenen jederzeit frei zu entscheiden, ob sie eine Unterstützungsleistung der Experten des CSN nutzen möchten oder nicht.

Digitaler Ersthelfer

Digitale Ersthelfer werden über das CSN in die Lage versetzt, Betroffene mit Ersthilfe bei der Behebung von kleineren IT-Störungen und IT-Sicherheitsvorfällen zu unterstützen. Hierfür stellt das CSN Digitalen Ersthelfern einen Leitfaden zur Verfügung, welchen sie zur Problemlösung heranziehen können. Die Vorfall-Bearbeitung erfolgt eigenständig durch Digitale Ersthelfer und unterliegt ausschließlich den Vereinbarungen zwischen ihnen und den Betroffenen. Ziel dieser Stufe ist es,

den Betroffenen Handlungsempfehlungen an die Hand zu geben. Sollten Digitale Ersthelfer ein Problem nicht beheben können, so haben Betroffene die Möglichkeit, sich an Vorfall-Praktiker oder IT-Sicherheitsdienstleister mit einem Team von Vorfall-Experten zu wenden.

Vorfall-Praktiker

Vorfall-Praktiker sind geschulte IT-Fachleute mit IT-Sicherheitserfahrung und einer zweitägigen Zusatzschulung incl. Prüfung. Sie unterstützen KMU telefonisch innerhalb ihrer Servicezeiten bei der Behebung von IT-Sicherheitsvorfällen und leisten so schnelle Ersthilfe.

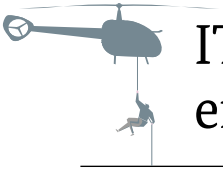
Die Aufgabe des Vorfall-Praktikers ist es eine qualifizierte Einschätzung und Analyse durchzuführen sowie Handlungsempfehlungen zu geben. Die Erkenntnisse werden in einem Vorfallbericht dokumentiert und den Unternehmen zugesandt.

Der Vorfall-Praktiker im eigenen Unternehmen

Zusätzlich existiert das Angebot des CSN an Unternehmen, deren Mitarbeiter auf einen IT-Sicherheitsvorfall vorzubereiten. Dazu können sich Mitarbeiter eines Unternehmens durch den Besuch einer Zusatzschulung zu „Unternehmens-Vorfall-Praktiker“ qualifizieren lassen. So verfügen diese Mitarbeiter über Kenntnisse, wie die Digitale Rettungskette aufgebaut ist und lernen das Vorgehen bei der Vorfallsbehandlung kennen. Bei einem IT-Sicherheitsvorfall ist es ihnen möglich, im Gleichklang und als Schnittstelle mit den Vorfall-Experten des CSN zu kommunizieren. Das Unternehmen kann hierdurch die Bedeutung des Themas „Notfallvorsorge“ in seinem Hause unterstreichen.

Vorfall-Experte

Vorfall-Experten sind in der Regel IT-Fachleute mit spezifischer Berufserfahrung, die sich zusätzlich im Rahmen einer Aufbauschulung für das CSN als Vorfall-Experte qualifiziert haben. Im Rahmen der Digitalen Rettungskette sollen sie soweit qualifiziert sein, dass sie in der Lage sind, den Vorfall tiefer zu analysieren und entsprechende Hilfeleistung zu geben – ggf. auch vor Ort. Für die Unterstützung durch Vorfall-Experten schließen die Betroffenen einen Dienstleistungsvertrag. Dieser wird selbständig und individuell zwischen beiden Parteien geschlossen. Das BSI nimmt hierauf keinen Einfluss, ebenso wenig wie auf die Vorfallsbearbeitung.



IT-Sicherheitsdienstleister mit einem Team von Vorfall-Experten

In den meisten Fällen kann davon ausgegangen werden, dass Vorfall-Experten die Probleme der Betroffenen lösen können. Sollte dies aber aufgrund der Komplexität von IT-Sicherheitsvorfalls oder der Netzwerkinfrastruktur nicht möglich sein, können Betroffene sich an die höchste Eskalationsstufe wenden, an zertifizierte und registrierte IT-Sicherheitsdienstleister. Diese halten ein Team aus Vorfall-Experten und Spezialisten vor, die aus diesem Grund auch komplexe IT-Sicherheitsvorfälle betreuen können. Auch in diesem Fall schließen die IT-Sicherheitsdienstleister mit den Betroffenen einen eigenständigen Dienstleistungsvertrag und legen den Umfang der Leistung fest. Das BSI ist auch hier nicht involviert und nimmt keinen Einfluss auf die Vertragsgestaltung oder die Durchführung der Vorfallsbearbeitung.

EXKURS:

Der für die Teilnehmer kostenfreie Basiskurs zum Digitalen Ersthelfern steht allen Interessierten und IT-affinen Personen offen. Es handelt sich hierbei um ein digitales Erste-Hilfe-Programm, welches in einem Onlinekurs vermittelt wird. Dabei erlernen die Teilnehmer im Selbststudium die Inhalte des „Leitfaden zur Reaktion auf IT-Vorfälle für Digitale Ersthelfer". Erst danach können sie sich bei Interesse im CSN registrieren lassen und die Leistung der Vorfallsbearbeitung über das CSN anbieten. Die Bedingungen, zu denen Digitale Ersthelfer ihre Hilfe gegenüber Betroffenen anbieten, insbesondere auch, ob diese kostenpflichtig ist, vereinbaren Digitale Ersthelfer und Betroffene selbstständig unter sich (Dienstleistungsvertrag). Das BSI nimmt hierauf keinen Einfluss, ebenso wenig wie auf die Durchführung der Vorfallsbearbeitung.

Die kostenpflichtige zweitägige Zusatzschulung inklusive Prüfungsworkshop für Vorfall-Praktiker bei den im CSN registrierten IT-Schulungsanbietern, basiert auf einem Curriculum, welches vom CSN bereitgestellt wird und dessen Themen in einem „Leitfaden zur Reaktion auf IT Sicherheitsvorfälle für Vorfall-Praktiker und Vorfall-Experten" aufbereitet sind. Danach ist eine Registrierung als Vorfall-Praktiker beim CSN möglich.

Um sich als Vorfall-Experten bei im CSN registrieren zu lassen, ist der Besuch einer dreitägigen Aufbauschulung erforderlich. Nach der Schulung schließt sich eine Personenzertifizierung durch die Zertifizierungsstelle des BSI an, die neben der Prüfung der Nachweise auch eine Kompetenzprüfung in Form eines Tests umfasst. Erst nach erfolgreicher Zertifizierung können sich Vorfall-Experten bei Interesse im Cyber- Sicherheitsnetzwerk registrieren lassen.

KONTAKTDATEN:

Cyber-Sicherheitsnetzwerk (CSN)
Bundesamt für Sicherheit in der Informationstechnik
Postfach 20 03 63
53133 Bonn

E-Mail: info@cyber-sicherheitsnetzwerk.de
Tel.: +49 800 - 2741000
Fax: +49 800 - 274600