SHD.
WIR BEWEGEN IT.

SHD Incident Response Team

Cyberangriff? Wir helfen.

Was ist das SHD Incident Response Team?

Bei einem IT-Sicherheitsvorfall sofort richtig zu handeln sowie mögliche Folgen zu beherrschen, ist ein klarer Geschäftsvorteil. Hier kommt unser Incident Response Team (IRT) ins Spiel: eine Gruppe von Fachexperten, die darauf spezialisiert ist, schnell und gezielt auf Cyberangriffe, Systemausfälle und Datenverletzungen zu reagieren.

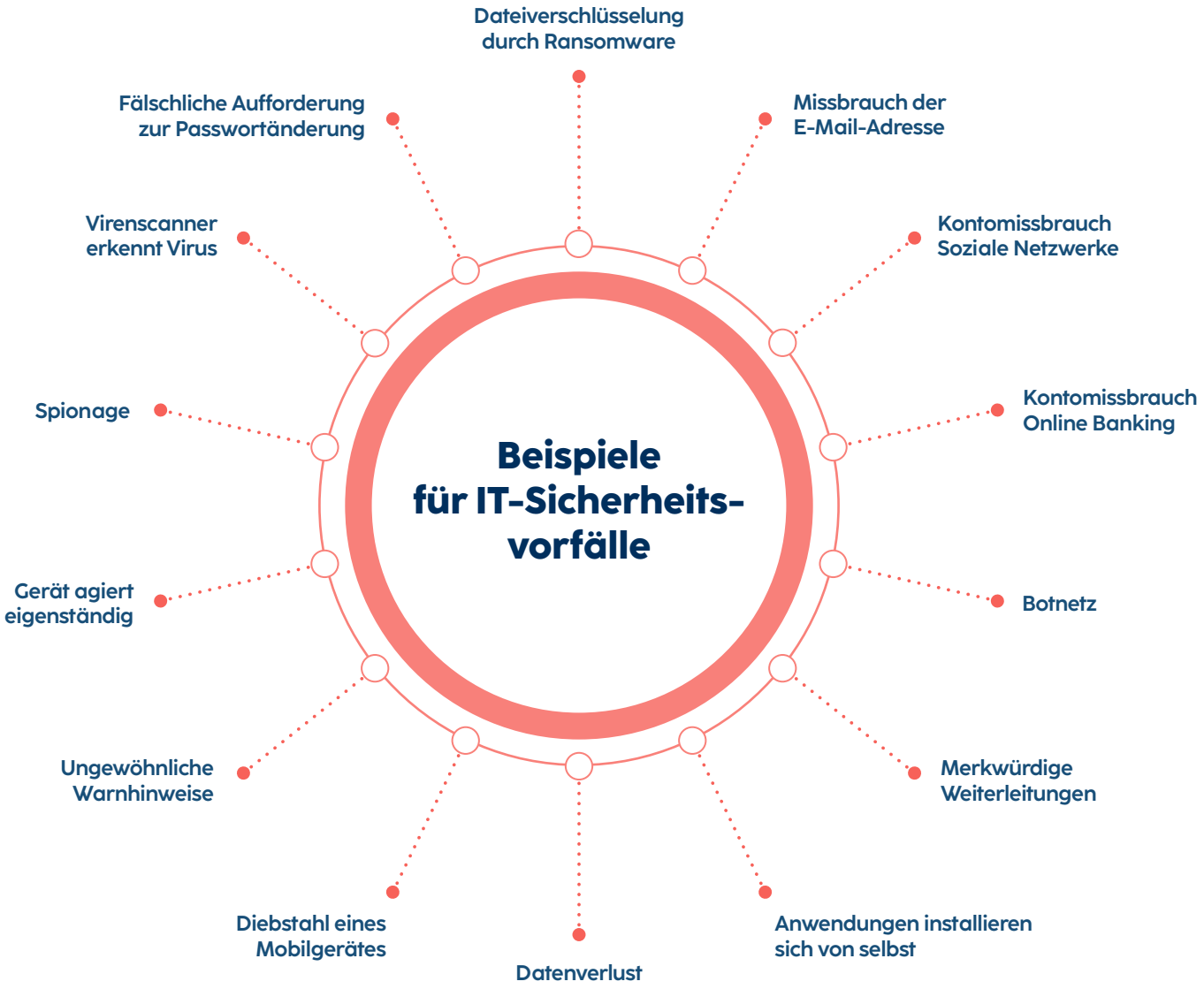
Auf Wunsch übernimmt das IRT von SHD den gesamten Umfang des Vorfalls, einschließlich der Vorbereitung, Reaktion und Wiederherstellung. SHD richtet sich dabei technologisch und organisatorisch nach den Vorgaben für APT-Response-Dienstleister im Sinne §3 BSIG und ist Mitglied im Cyber-Sicherheitsnetzwerk des Bundesamtes für Sicherheit in der Informationstechnik (BSI).

SHD ist Mitglied des DIRT.

Das Deutsche Incident Response Team (DIRT) stellt ein deutschlandweites Netzwerk für die IT-Cyberkrisen-Bewältigung dar. Es besteht aus über 50 BSI-Vorfall-Experten und 4.500 IT-Spezialisten in allen Bereichen. Dank regionaler mobiler Notfall-Rechenzentren kann das Netzwerk aus Einsatzleitern und IT-Forensikern schnell vor Ort Hilfe bei der IT-Wiederherstellung leisten.

Störung oder Sicherheitsvorfall – wo liegt der Unterschied?

	IT-Störung (Malfunction)	IT-Sicherheitsvorfall (Major Security Incident)
Ursache	technischer Defekt, unbeabsichtigtes (menschliches) Fehlverhalten	kriminelle Cyberangriffe
Einwirkung Dritter	nein	ja
Beeinträchtigung / Ausfall	kurzzeitig	langwierig
Behandlungsaufwand	gering	hoch



MAJOR INCIDENT – was tun?

1. Ruhe bewahren

Bleiben Sie in Krisensituationen ruhig und bewerten Sie die Situation sachlich, um überstürzte Entscheidungen zu vermeiden. Lehnen Sie die Zahlung von Lösegeld ab, da dies keine Garantie für eine Problemlösung darstellt, zukünftige Angriffe fördern könnte und in vielen Fällen sogar eine Straftat darstellt.

2. Response-Team bilden

Stellen Sie ein spezialisiertes Team aus IT-Sicherheitsexperten (inhouse oder extern) zusammen, um eine koordinierte Reaktion auf den Vorfall zu gewährleisten. Die enge Zusammenarbeit dieses Teams garantiert dabei schnelle und effektive Maßnahmen.

3. Notfall-Server nutzen

Um den Betrieb aufrechtzuerhalten und Datenverlust zu minimieren, schaltet das Team auf Notfall-Server um (falls bei Ihnen vorhanden). Diese Server sind bereits vorbereitet und werden regelmäßig aktualisiert, um im Notfall eine schnelle Wiederherstellung zu ermöglichen.

4. Sicherheitslücke isolieren

Das Response-Team identifiziert und isoliert die betroffenen Systeme, um eine weitere Ausbreitung des Vorfalls zu verhindern. Dabei werden Backup-Geräte getrennt und betroffene Geräte vom Netzwerk isoliert.

5. Vorfall untersuchen

Eine gründliche Untersuchung wird durchgeführt, um die Ursache des Vorfalls zu ermitteln und zu verstehen, wie der Angriff erfolgte. Dies umfasst die Analyse von Log-Dateien, Systemkonfigurationen und anderen relevanten Daten.

6. Prozess dokumentieren

Jeder Schritt des Response-Teams wird sorgfältig festgehalten, damit der Vorfall nachvollziehbar bleibt und für zukünftige Referenzen daraus gelernt werden kann. Diese Dokumentation beinhaltet Details über ergriffene Maßnahmen, festgestellte Schwachstellen und erzielte Ergebnisse.

7. Betroffene kontaktieren

Das Team informiert alle betroffenen Parteien über den Vorfall – einschließlich Mitarbeiter, Kunden und Partner. Diese Kommunikation erfolgt klar, transparent und schnell, um Vertrauen zu bewahren und die Betroffenen über notwendige Schritte in Kenntnis zu setzen.

8. Vorsorge betreiben

Entwickeln Sie Maßnahmen auf Basis der Vorfallerkenntnisse, um ähnliche Incidents in Zukunft zu verhindern – zum Beispiel durch die Verbesserung von Sicherheitsprotokollen oder regelmäßige Schulungen für Mitarbeiter. Ziehen Sie bei Bedarf externe Sicherheitsspezialisten für diese Maßnahmen hinzu.

Darum kümmert sich unser IRT

Für die professionelle Analyse stellt unser Response-Team die passende Hardware bereit – von der Monitoring-Firewall zur Prüfung des Netzwerkverkehrs über eine Forensik-Workstation zur leistungsfähigen Beweis-Auswertung bis hin zum Notfall-Laptop, der zu Konfigurationszwecken an die betroffene Umgebung angeschlossen werden kann.

Unser Team für Ihre Sicherheit

Einsatzleiter

Der Einsatzleiter übernimmt die Leitung des Incident-Response-Teams. Er hilft bei der Bewältigung der Krisensituation sowie bei der Koordination von Forensik, Bereinigung und Wiederanlauf. Der Einsatzleiter ist verantwortlich für die enge Zusammenarbeit und Kommunikation mit weiteren Dienstleistern, Kunden, Versicherungen und Behörden.

Security Consultant

Der Security Consultant unterstützt Kunden in der Anforderungsanalyse, beim Design sowie der Implementierung von komplexen Cyber-Security-Lösungen. Er identifiziert Schwachstellen im Unternehmen, entwickelt geeignete Gegenmaßnahmen und setzt diese um.

Forensiker

Der IRT-Forensiker führt forensische Analysen und Untersuchungen von betroffenen Systemen durch. Er sammelt digitale Beweise und erstellt lückenlose Berichte für das Management und gegebenenfalls für juristische Zwecke.

Die Leistungspakete im Überblick

Die Meldung eines Sicherheitsnotfalls ist 24/7 möglich – die Zusage für einen spontaner IRT-Einsatz erfolgt nach individueller Prüfung. Die Bereitstellung eines Response-Teams kann im Rahmen eines Service-Vertrags zugesichert werden. Sprechen Sie uns an: **kontakt@shd-online.de**

SHD IR Service S	SHD IR Service M	SHD IR Service L
24/7 Erreichbarkeit der IRT-Hotline, um einen Fall zu melden	24/7 Erreichbarkeit der IRT-Hotline, um einen Fall zu melden	24/7 Erreichbarkeit der IRT-Hotline, um einen Fall zu melden
Telefonische Erstberatung (24/7, innerhalb 4h): Annahme, Vorqualifikation von Verdachts-, Vor-, und Notfällen	**Telefonische Erstberatung (24/7, innerhalb 4h): Annahme, Vorqualifikation von Verdachts-, Vor-, und Notfällen**	**Telefonische Erstberatung (24/7, innerhalb 4h): Annahme, Vorqualifikation von Verdachts-, Vor-, und Notfällen**
SHD Incident Response: Next Business Day remote oder vor Ort	**SHD Incident Response: Next Business Day remote oder vor Ort**	**SHD Incident Response: Next Business Day remote oder vor Ort**
Abrechnung nach Aufwand	**inkl. 50h IR-Leistungen/Jahr, danach Abrechnung nach Aufwand, Umwandlung in Security-Leistungen (max. 25h/Jahr)**	**inkl. 100h IR-Leistungen/Jahr, danach Abrechnung nach Aufwand, Umwandlung in Security-Leistungen (max. 50h/Jahr)**
inkl. halbjährlicher Jour-Fixe-Termin	inkl. halbjährlicher Jour-Fixe-Termin	inkl. halbjährlicher Jour-Fixe-Termin
Bereitstellung eines IR-Teams, bestehend aus Einsatzleiter und Security Analysten/Forensiker	Bereitstellung eines IR-Teams, bestehend aus Einsatzleiter und Security Analysten/Forensiker	Bereitstellung eines IR-Teams, bestehend aus Einsatzleiter und Security Analysten/Forensiker
zzgl. Bereitstellung SHD-Equipment	zzgl. Bereitstellung SHD-Equipment	zzgl. Bereitstellung SHD-Equipment

Mehr Sicherheit: Soweit im Paket vorgesehen kann die Hälfte des ungenutzten Stundenkontingents nach Ablauf eines Vertragsjahres innerhalb von 3 Monaten in sicherheitsnahe SHD-Dienstleistungen (z.B. Penetrationstests, Security Consulting, Audits o.ä.) umgewandelt werden.

Mehr Support: Beim Wiederaufbau Ihrer Systeme unterstützt Sie SHD auf Wunsch mit den entsprechenden Spezialisten: Microsoft AD, Microsoft Exchange, Backup, Virtualisierung, Netzwerk & Firewall.

Sie benötigen sofortige Hilfe?

Für die initiale Meldung eines Vorfalls erreichen Sie unser IRT werktags, Mo–Fr von 8–17 Uhr unter:

0800-743 0478*

vorfall@shd-online.de

* kostenlos aus dem dt. Fest- und Mobilfunknetz

SHD.

Vorsorge statt Ernstfall: zusätzliche Leistungen von SHD

IT- & Organisations-Check:

Wir führen eine fundierte Analyse und Bewertung Ihres IT-Betriebs vor dem Hintergrund zentraler Service- und Geschäftsprozesse durch. Aus Basis vorab definierter, wichtiger IT- und Servicekomponenten in Ihrem Unternehmen können bestehende Strukturen gezielt bewertet werden. Gemeinsam mit Ihnen erarbeiten wir Handlungsempfehlungen und Optionen für eine leistungsfähigere IT-Umgebung. Unser standardisiertes Verfahren liefert bereits innerhalb von 4 bis 8 Tagen konkrete Vorschläge, in welchen Bereichen weiteres Potenzial besteht und welche IT-Infrastruktur- und Servicekomponenten besonderer Aufmerksamkeit bedürfen.

ISMS & BCMS:

Die Identifizierung, Bewertung und Kontrolle von Sicherheitsrisiken ist essenziell. Wir helfen Ihnen dabei, Gefahren zu minimieren, die zu Datenverlust oder Datenkompromittierung führen könnten oder Ihre Geschäftskontinuität bedrohen. Wir unterstützen Sie bei der Vorbereitung auf unerwartete kritische Ereignisse und sorgen dafür, dass Sicherheitsvorfälle effizient adressiert werden und Ihre Organisation in der Lage ist, kritische Geschäftsprozesse aufrechtzuerhalten.

SOC Services:

Nutzen Sie das Security Operations Center von SHD als Ihre Sicherheitsleitstelle, die sich um den Schutz der IT-Infrastruktur Ihres Unternehmens kümmert. Im SOC werden sicherheitsrelevante Systeme überwacht – dazu zählen vor allem das Unternehmensnetzwerk, die Server oder Internetservices. Unser Team untersucht Systeme und Log-Dateien auf Unregelmäßigkeiten, schlägt bei Sicherheitsvorfällen Alarm und leitet sofortige Gegenmaßnahmen ein.

Penetration Tests:

Mit individualisiertem Pentesting bietet Ihnen SHD die Möglichkeit, gezielt technische Sicherheitslücken in Ihrem Unternehmen aufzuspüren und konkrete Maßnahmen abzuleiten. Unser Fokus liegt dabei auf verständlichen Lösungen, die zu Ihren angestrebten Schutzzielen und zu Ihren verfügbaren Ressourcen passen.

SHD ist Ihr zuverlässiger Ansprechpartner für schnelle professionelle Hilfe bei Sicherheitsnotfällen. Dank Mitgliedschaft im Deutschen Incident Response Team (DIRT), langjähriger Erfahrung und großem Herstellernetzwerk unterstützen wir die Sicherstellung Ihres IT-Betriebs gesamtheitlich.

Fordern Sie uns, wir überzeugen Sie!

SHD.
WIR BEWEGEN IT.

Zertifiziert nach
ISO 9001 und ISO 27001

- 1990 in Dresden gegründet
- Stammhaus in Dresden, Geschäftsstellen in Berlin, Leipzig, Hamburg, Nürnberg und in der Lausitz
- Spezielle Lösungen für KRITIS-Anforderungen
- Wir bewegen die IT im Industrie-, Krankenhaus- u. Energiesektor sowie in öffentlichen Einrichtungen

GESCHÄFTLICHE SCHWERPUNKTE

- Digitale Transformation
- IT-Infrastruktur Services
- IT-Sicherheit
- Professioneller IT-Service
- Managed und Cloud Services

KONTAKT: SHD System-Haus-Dresden GmbH · info@shd-online.de · www.shd-online.de

550-2.4-05.TFR