CSIRT as a Service / CSIRT Rapid Response

Kein Unternehmen ist gegen Sicherheitsvorfälle immun. Die Behandlung solcher Vorfälle erfordert spezialisierte Cybersecurity Incident Response Teams (CSIRT), analog zur Feuerwehr bei einem Brand.

Die hohe Vernetzung und die steigende Komplexität moderner Unternehmen erhöht die Angriffsfläche drastisch – und damit das Risiko, von einer erfolgreichen Cyberattacke getroffen zu werden.

Was ist CSIRT as a Service/Rapid Response?

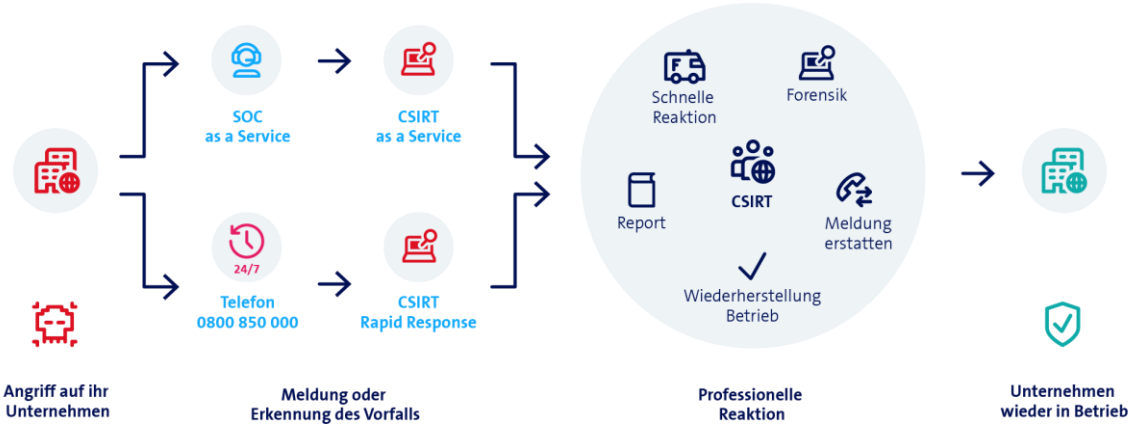
Security Incidents können einen signifikanten Business Impact haben und leider nicht immer verhindert werden. Entscheidend ist dann die schnelle und professionelle Reaktion durch ein Cybersecurity Incident Response Team, kurz CSIRT.

Das Team übernimmt den Lead bei einem verifizierten Security Incident und unterstützt den Kunden bei der Reaktion auf den Vorfall sowie bei der Beseitigung von Schadsoftware und der Wiederherstellung des operativen Betriebs. Die Basisleistung ist in zwei Ausprägungen erhältlich.

Ihre Nutzen mit CSIRT as a Service/Rapid Response

- Schnelle Antwort auf Cyberangriffe
  Bei Sicherheitsvorfällen schnell und professionell reagieren.
- Profitieren von der Expertise und Erfahrung unserer Security-Fachleute
  Bestens ausgebildete Security-Spezialist*innen mit breiter und langjähriger Erfahrung.
- Detaillierte Sicherheitsüberprüfung von kompromittierten Systemen
  Schnelle Analyse der Angriffsvektoren und die Eingrenzung betroffener Systeme.
- Unterstützung bei der Wiederherstellung des ordentlichen Betriebs
  Unterstützung, um die betroffenen Systeme wieder in die Produktivumgebung zu integrieren.

So funktioniert CSIRT as a Service / Rapid Response



swisscom

Facts & Figures

Basisleistungen	CSIRT as a Service mit Servicevertrag und SLA: Zur Analyse und Bewältigung ziehen Sie Experten von Swisscom bei. Wir leiten den Security-Incident-Management-Prozess remote oder bei Ihnen vor Ort, unterstützen Sie bei der Beweissicherung sowie der Kommunikation mit Kunden und Partnern.
	CSIRT Rapid Response ohne SLA: Rapid Response ist mit der Basisleistung von CSIRTaaS vergleichbar. Im Unterschied dazu melden Sie sich bei einem Vorfall über die Nummer 0800 850 000, dies ganz ohne Servicevertrag. Es gibt jedoch keine garantierte Reaktionszeit. Ein Onboarding, das bei CSIRT as a Service initial durchgeführt wird, steht direkt vor dem Einsatz an. Zusätzlich fällt eine Einsatzpauschale an und die Stundensätze sind höher kalkuliert.
Optionale Leistunge	Abschlussbericht nach individueller Kundenvorgabe und im gewünschten Design in Deutsch oder Englisch.
	Zusätzliche Analysen ausserhalb des Security-Incident-Management-Prozesses (z.B. Attribution, Aufgleisung Strafverfolgung usw.).
	Vorsorgliche Überprüfung nicht direkt betroffener Systeme.
	Beweissicherung zur straf-, zivil- und öffentlichrechtlichen Verwendung in der Schweiz.
	File Analysis Solution (nur für Outsourcing-Kunden), direkter Zugriff auf Kundendateien für tiefgreifende Analysen. Ohne diese Option kann Swisscom als Provider gemäss Unternehmensrichtlinie nicht direkt auf Kundendateien zugreifen.
Zusatzservices	Security Analytics as a Service (SAaaS): Wir sind Fachleute in den Themen Security und Big Data und stellen Ihnen unsere bewährte Security-Analytics-Infrastruktur zur Verfügung. Schliessen Sie weitere Logquellen aus der Cloud, On-Premises oder von einem Managed Provider an und erhalten Sie im Dashboard einen Überblick über potenzielle Sicherheitsvorfälle. Analyse und Reaktion auf Sicherheitsvorfälle übernehmen Sie selbst.
	SOC as a Service (SOCaaS): Sie erhalten via Dashboard einen Überblick über potenzielle und bestätigte Sicherheitsvorfälle aus definierten Logdaten Ihrer Unternehmung sowie Analysen mit konkreten Handlungsempfehlungen. Auf kritische Security Incidents reagieren Sie selbständig.
	Network Detection and Response as a Service (NDRaaS): Wird als Erweiterung zu den statischen Erkennungsmöglichkeiten von SAaaS durch eine dynamische Threat Detection basierend auf Machine-Learning-Modellen unterstützt. Der Service wird zusammen mit einer Partnerfirma erbracht. Der Mehrwert ergibt sich in den Bereichen Web (Proxy) und Netzwerk (DNS, Netflow und Firewall-Traffic-Daten), was maximale Visibilität erlaubt.
	Digital Risk Protection as a Service (DRPaaS): Sie werden proaktiv informiert über das Vorkommen von sensiblen Geschäfts- und persönlichen Informationen Ihres Unternehmens in öffentlichen und geschlossenen Netzen (z.B. Darknet). Unsere Handlungsempfehlungen für bestätigte Sicherheitsvorfälle setzen Sie selbständig um.
	Wiederaufbau der IT-Infrastruktur nach Kundenvorgaben durch unsere erfahrenen Infrastrukturspezialist*innen.

Mehr Informationen und den Kontakt zu unserem Experten finden Sie auf **swisscom.ch/csirt**

Swisscom (Schweiz) AG Geschäftskunden, Postfach,
CH-3050 Bern, Tel. 0800 800 900, www.swisscom.ch/enterprise

swisscom