Orange Cyberdefense

Das Orange Cyberdefense
CSIRT

Seien Sie vorbereitet: Incident Response Services

Das Orange Cyberdefense Cybersecurity Incident Response Team (CSIRT) ist ein europäisches Eliteteam, das proaktive Beratung, Reaktion auf Vorfälle und technische Beratung anbietet, um Kunden bei der Bewältigung eines Sicherheitsvorfalls von der ersten Erkennung bis zur Behebung zu unterstützen.

Der Fokus der Aufmerksamkeit

Früher gab es nur wenige Medienberichte über große Datenschutzverletzungen, die im Technikteil der Nachrichten oder in speziellen Branchenzeitungen versteckt waren. Die Realität sieht nun so aus, dass Datenschutzverletzungen zu den Mainstream-Nachrichten gehören und ein wahrer PR-Alptraum zusätzlich zum eigentlichen Schaden sind.

Der Schlüssel zur Abmilderung der Auswirkungen von Cyber-Sicherheitsvorfällen ist die Zeit zwischen Erkennung und Reaktion. Vielen Unternehmen fehlen die Infrastruktur, die Prozesse und die Mitarbeiter, die für eine schnelle und sichere Reaktion erforderlich sind. Die Incident Response Services von Orange Cyberdefense ermöglichen es jedem Unternehmen, unser CSIRT als Erweiterung des eigenen Sicherheitsteams in Anspruch zu nehmen. Unser Team steht rund um die Uhr zur Verfügung und ermöglicht es Ihnen, Ihre vorhandenen Ressourcen mit erfahrenen, vielseitig qualifizierten Spezialisten für digitale Forensik und Incident Response zu ergänzen.

Über das Orange Cyberdefense CSIRT:

- Teil des Orange Cyberdefense CERT, mit einem erweiterten Team von mehr als 80 Personen weltweit
- Großes, vielseitiges CSIRT-Team mit mehr als 20 Einsatzkräften in West-, Nord- und Mitteleuropa
- Mitglieder der von der Industrie anerkannten Gremien für Incident Response, einschließlich CREST, TF-CSIRT, FIRST und ENISA
- Hochgradig erfahrenes Team mit Erfahrung im Umgang mit Angriffen auf nationaler Ebene
- Anerkennung durch Analysten wie Gartner* und Forrester**

Wir helfen Ihnen bei der Bewältigung des gesamten Vorfalls, von einem einfachen Verstoß gegen eine Richtlinie bis hin zu einer unternehmensweiten Kompromittierung, wobei wir als wichtiger Bestandteil des Incident Response-Plans Ihrer Organisation und als Kollege innerhalb Ihres eigenen Incident Response Teams arbeiten. Das CSIRT folgt den Grundsätzen des „Association of Chief Police Officers' (ACPO) Good Practice Guide for Computer-based Electronic Evidence" für alle Aspekte der Beweisführung, unabhängig von den kriminellen Umständen oder der Beteiligung der Strafverfolgungsbehörden.

* Representative Vendor, Gartner Market Guide for Digital Forensics and Incident Response Services, December 2019
** Forrester NowTech report for European Cybersecurity Incident Response Services, Q1 2020

Sobald eine Sicherheitsverletzung erkannt wird, ist es von entscheidender Bedeutung zu wissen, wie zu reagieren ist. Sie benötigen in der Regel:

Expertise

Erfahrung und Fähigkeiten spielen vor allem bei der Reaktion auf kritische Cybersicherheitsvorfälle eine Rolle. Das CSIRT verfeinert und aktualisiert kontinuierlich seine Methoden und Techniken. Dies ermöglicht es unseren Teams, Sicherheitsvorfälle vertrauensvoll und effizient zu behandeln. Wir nutzen unser gebündeltes Wissen, um Kunden bei der Erkennung, Eindämmung, Behebung einer Reihe von Vorfällen und der Wiederherstellung danach zu helfen.

Zuverlässigkeit

Angesichts der immer strenger werdenden Vorschriften wie GDPR und dem aufstrebenden Markt für Cybersecurity-Versicherungen, die eine immer schnellere Bewertung und Meldung von Vorfällen erfordern, ist ein solider Partner, der die erforderliche Expertise bereitstellen kann, von entscheidender Bedeutung. In der für die meisten Unternehmen größten Stunde der Not brauchen Sie jemanden, dem Sie vertrauen können.

Vorbereitung

Proaktive Dienste helfen Ihnen bei der Planung, Vorbereitung, Schulung und Prüfung Ihrer Mitarbeiter, Prozesse und Technologien, so dass Sie im Falle eines Vorfalls vorbereitet und souverän sind und bewährte Methoden zur Steuerung der Reaktion einsetzen. Das Orange Cyberdefense CSIRT hilft Ihnen, so gut wie möglich vorbereitet zu sein. Wir wissen, was funktioniert und – was noch wichtiger ist – was nicht funktioniert.

Hier finden Sie die Incident Response Hotline:
orangecyberdefense.com/de/incident-response-hotline/

Vorteile:

- Qualitativ hochwertige Reaktion auf Vorfälle, wenn Sie sie brauchen (auf Abruf oder auf Vertragsbasis).
- Entwickelt Ihre internen Fähigkeiten, Dokumentationen und Prozesse, damit Sie auf ein breites Spektrum von Vorfällen vorbereitet sind.
- Zugang zu einem anpassungsfähigen, kundenorientierten Team, das leidenschaftlich an das glaubt, was es tut.
- Zugang zu Fachkenntnissen in verschiedenen Bereichen, mit einem der größten CSIRT-Teams in Europa sowie Zugang zum breiteren CERT-Team, alles untermauert durch unseren Intelligence-gestützten Sicherheitsansatz.

Die Zusammenarbeit mit uns

Unser CSIRT bietet alle wichtigen Komponenten für eine erstklassige Incident Response:

Technische Erfahrung
Es ist wichtig, über erfahrene Responder zu verfügen, die sich, auch unter hohem Druck stehend, wohlfühlen und souverän damit umgehen können. Die CSIRT-Mitglieder von Orange Cyberdefense haben mit einigen der größten Unternehmen der Welt zusammengearbeitet und auf einige der verheerendsten und bekanntesten Cyberangriffe der letzten Jahre reagiert, darunter Petya und WannaCry.

Wissen
Orange Cyberdefense kennt Ihr Unternehmen. Unsere Retainer-Services für die Reaktion auf Vorfälle umfassen einen Workshop zur Risikobewertung, um sicherzustellen, dass unser Team einen detaillierten Überblick über die aktuelle Situation hat, um ein Maximum an Einblick zu gewinnen, noch bevor eine Reaktion erforderlich ist.

Intelligence-led Incident Response
Wir sammeln Anhaltspunkte für eine Gefährdung (Indicators of Compromise, IOCs) aus dem Orange Cyberdefense Threat Intelligence Backbone. Unser CSIRT ist eng mit dem Rest des CERT (einschließlich unseres Cybercrime Monitoring Teams) und unserem Netzwerk von SOCs und CyberSOCs verbunden. Die Informationen, die in das CSIRT einfließen und es verlassen, nutzen die uns zur Verfügung stehenden Informationen über Cyber-Bedrohungen in vollem Umfang und ermöglichen es uns, bessere Ratschläge für die Vorbereitung auf künftige Vorfälle zu geben und einen gezielten Kontext für einen Vorfall zu liefern.

Eindämmung
Angesichts der Ausbrüche von Ransomware und anderer bösartiger Malware, die alle Branchen bedrohen, ist eine Eindämmung von entscheidender Bedeutung. Das CSIRT-Team hat in jahrelanger IR-Arbeit ein Toolkit für die Reaktion auf Vorfälle entwickelt, das ständig weiterentwickelt wird, um sicherzustellen, dass die Bedrohung schnell eingedämmt, die Quelle identifiziert und der Schaden auf ein Minimum begrenzt wird, wenn Ihre Verteidigungsmaßnahmen durchbrochen wurden.

Ein proaktiver Ansatz
Es ist wichtig, nicht zu warten, bis ein Cybersecurity Incident eintritt. Übung macht den Meister und Absicherung ist der Schlüssel. Unser CSIRT bietet Dienstleistungen an, um auf das Schlimmste vorbereitet zu sein – von der Beratung bei der Reaktion auf Vorfälle, wie der Entwicklung von Reaktionsplänen und Tabletop-Übungen, bis hin zu Compromise Assessments, die proaktiv nach Anzeichen eines Eindringens suchen, die zuvor unentdeckt geblieben sind.

Retainer
Es ist wichtig, dass Sie eine Garantie für qualitativ hochwertige Kompetenzen haben, wenn Sie sie am meisten brauchen; Vorbereitung ist der Schlüssel. Das Orange Cyberdefense CSIRT steht Ihnen auf Honorarbasis rund um die Uhr an 365 Tagen im Jahr mit einer garantierten Remote- und Vor-Ort-Responder-SLA zur Verfügung. Unsere Retainer-Services sind so konzipiert, dass ungenutzte Stunden für proaktive Aufgaben wie Tests, Schulungen und Prozessüberprüfungen genutzt werden können.*

*Je nach Servicelevel

Mehr Infos finden Sie auf
www.orangecyberdefense.de

Orange Cyberdefense
Paul-Gerhardt-Allee 24, 81245 München

info@de.orangecyberdefense.com
+49 89 2000148 00