CYBER SECURITY INCIDENT RESPONSE

Kompetente Unterstützung zu jeder Zeit

SICHERHEITSVORFALL – WAS NUN?

UMFASSENDER SCHUTZ

Täglich werden weltweit hunderte von Unternehmen angegriffen und nachhaltig geschädigt. Medien überschlagen sich mit immer hochtrabenderen Schlagzeilen. Cyber-Angriffe werden ausgeklügelter und gezielter.

In Zeiten wie diesen ist es eine wahre Herausforderung in dieser vernetzten Welt, welche von raschen Innovationszyklen geprägt ist, eine Organisation nachhaltig sicher zu gestalten. Es gibt keine Patentlösung um Systeme oder Daten abzusichern. Stattdessen wird eine vielschichtige Sicherheitsstrategie unabdingbar. Eine solche Strategie muss sich mit dem Ernstfall auseinander setzen.

MOTIVATOREN

- Die Anzahl der Cyber Security Incidents erhöht sich stetig.
- Die Anzahl der Unternehmen, welche von Cyber Security Incidents betroffen sind, erweitert sich stetig.
- Neue rechtliche Anforderungen und Best Practises haben einen hohen Einfluss darauf wie sich Unternehmen schützen müssen.
- System- und Netzwerkadministratoren können die Organisation nicht alleine vor Schaden durch Cyber Security Incidents bewahren.
- Holistische Betrachtungen von Informationssicherheit fordern wirksame Behandlung von Sicherheitsvorfällen.

T · · Systems ·

„FIREFIGHTING“ RICHTIGES HANDELN - WENN JEDE MINUTE ZÄHLT

UNSERE VORGEHENSWEISE

Unser erster Schritt ist eine Analyse der Situation um Fakten und mögliche Ursachen zu sammeln. Auf Basis dieser Analyse wird ein priorisierter Plan erstellt und Aufgaben werden verteilt. In stetiger Rücksprache mit dem Management wird für rasche Entscheidungsfindung und die notwendige Handlungsfähigkeit gesorgt.

T-Systems behandelt Incidents nach einem klar strukturierten Prozess, um eine rasche und geordnete Behandlung ihres Zwischenfalls zu gewährleisten.

PROZESS IM ÜBERBLICK

Vorbereitung: Gewährleisten von technischen Rahmenbedingungen, sowie organisatorische Verankerung.

Identifikation: Rasche Identifikation, Kategorisierung und Eskalation von Vorfällen.

Eindämmung: Maßnahmen um weitere Verbreitung und Schäden zu verhindern; Eindämmung des Schadensausmaßes.

Säuberung: Bereinigung aller betroffenen Systeme und Kontrolle der Effektivität der Säuberungsmaßnahmen.

Wiederherstellung: Geregelte Zurückführung des Betriebs in den Tagesbetrieb; Formelles Ende des Incidents.

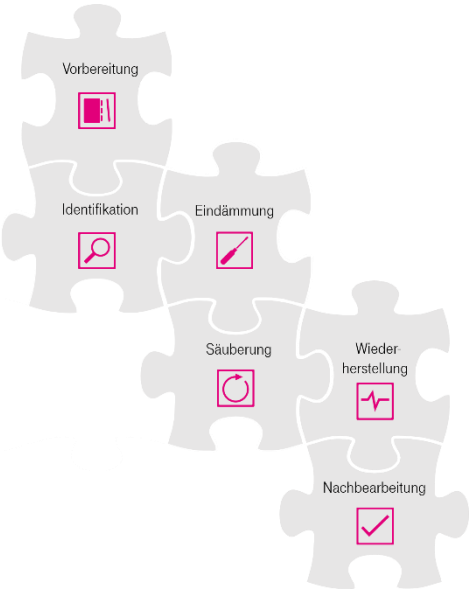
Nachbearbeitung: Dokumentation des Zwischenfalles; Einleitung von Maßnahmen zur nachhaltigen Verbesserung der Sicherheit.

ALLZEIT BEREIT

T-Systems verfügt über viele Jahre Erfahrung im Betrieb hochkomplexer IT-Landschaften. Mit dem Security Operations Center steht eine 7x24 besetzte und erreichbare Service-Stelle zur Verfügung, die Sie im Fall von Sicherheitsvorfällen unterstützt und Vorfälle bewertet.
Diese Erfahrungswerte sind ihr direkter Vorteil, denn Sie können zu jeder Tages- und Nachtzeit auf ein Team von Experten zurückgreifen.

THREAT INTELLIGENCE

Wissen ist Macht!
Im Sinne dieser alten Weisheit informiert sich T-Systems stetig über aktuelle Entwicklungen und Bedrohungen im Cyberspace. Genau dieses Wissen wollen wir teilen und Ihnen regelmäßige, einfach und klar aufgebaute Informationen liefern, um Sie bei Ihrer Entscheidungsfindung zu unterstützen. Wir helfen Ihnen Ihr Lagebild zu erstellen.



DAS WICHTIGSTE AUF EINEN BLICK.

- 24 / 7 Bereitschaft.
- Sicherheitsexperten mit langjähriger Erfahrung mit der Behandlung von Vorfällen.
- Threat Intelligence – Regelmäßige, klar verständliche Nachrichten aus der Cyber Security Welt.
- Breites Fachwissen und Verfügbarkeit von Experten.
- Klare Kostenstruktur.
- Unkomplizierter Abruf.
- Professionell und vertraulich.

HABEN SIE NOCH FRAGEN?
Internet: www.t-systems.de/security
oder schreiben Sie eine E-Mail an
security-info@t-systems.at

EXPERTENKONTAKT
T-Systems Austria GesmH
Martin Krumböck
martin.krumboeck@t-systems.at

HERAUSGEBER
T-Systems Austria GesmbH
Rennweg 97-99
1030 Wien