10.09.2024 – 13:53 Uhr

Cyberangriff vorprogrammiert? So erstellen Sie einen effektiven Incident Response Plan (IRP)

Kaiserslautern (ots) -

Cyber-Attacken treffen Organisationen immer häufiger und meist unerwartet. Prominente Beispiele wie die Log4J-Sicherheitslücke 2021 zeigen: Eine Krise kann plötzlich eintreten und sofortiges, koordiniertes Handeln erfordern. Doch wie können Unternehmen sicherstellen, dass in solchen Momenten die richtigen Maßnahmen ergriffen werden und die Mitarbeiter nicht in Panik geraten? Die Antwort liegt in einem Incident Response Plan (IPR).

Cybersicherheit: Früher an später denken

Der ITSM-Tool-Anbieter TOPdesk beschäftigt sich intensiv mit Fragen des Krisenmanagements, um auf mögliche Cyber-Angriffe vorbereitet zu sein. "Die Erfahrungen unseres Krisenmanagement-Teams zeigen: Ohne einen vorbereiteten Plan wird eine Cyber-Attacke schnell zu einer chaotischen Situation.", so Martin Stephan, Sicherheitsbeauftragter bei TOPdesk. "Panik und Unsicherheit breiten sich aus, die betroffenen Personen verlieren den Überblick und die Reaktionszeit wird unnötig verlängert."

Ein Incident Response Plan, im deutschsprachigen Raum auch als Vorfallreaktionsplan bekannt, schafft hier Abhilfe. Er beschreibt präzise, was bei einem Sicherheitsvorfall zu tun ist und sorgt dafür, dass im Ernstfall keine wertvolle Zeit verloren geht.

Warum ein Incident Response Plan (IRP) unerlässlich ist

Nach einem Vorfall, wie einer Ransomware-Attacke, läuft die Uhr gegen die Organisation. Sie haben oft nur 72 Stunden Zeit, um eine Datenschutzverletzung an die zuständige Behörde zu melden. Diese Frist vergeht schnell, während gleichzeitig Systeme gesichert, Mitarbeiter informiert und das Ausmaß des Angriffs festgestellt werden muss. Ein gut ausgearbeiteter IRP legt genau fest, welche Schritte wann zu erfolgen haben, und hilft so, Zeitdruck und Fehler zu minimieren.

So wird ein Incident Response Plan erstellt

Ein Incident Response Plan sollte auf die spezifischen Bedürfnisse der Organisation abgestimmt sein. Es ist ratsam, zunächst ein Krisenmanagement-Team zusammenzustellen, das aus Mitgliedern verschiedener Abteilungen besteht. Diese sollten über detaillierte Kenntnisse der Unternehmensstruktur verfügen, einen kühlen Kopf bewahren und in Krisenzeiten gut erreichbar sein. Bei TOPdesk etwa gibt es ein zehnköpfiges Team, das alle sechs Monate hypothetische Krisensituationen durchspielt, um auf echte Vorfälle vorbereitet zu sein.

Ein weiterer wichtiger Schritt ist die Integration von Alarmierungssystemen. Dies lässt sich beispielsweise via "Panik-Knopf" im Self Service Portal für die Mitarbeiter*innen lösen. Kam es zu einer erfolgreichen Phishing-Attacke, kann die betroffene Person mit nur einem Klick einen Workflow anstoßen, durch welchen das Krisenmanagement-Team (international auch bekannt als CMT/Crisis Management Team) sofort per Microsoft Teams und bei Bedarf zusätzlich per SMS benachrichtigt wird. So kann jeder Vorfall ohne Zeitverlust gemeldet und bearbeitet werden.

Effiziente Kommunikation und Dokumentation

Ein guter IRP sollte immer auch klare Kommunikationsstrategien enthalten. Besonders bei größeren Vorfällen ist es wichtig, dass alle Beteiligten zeitnah und präzise informiert werden. "Wir setzen hier auf die Einrichtung eines Major Incident und die Erstellung von Wissensartikeln, die allen betroffenen Mitarbeitern jederzeit zugänglich sind.", erklärt IT-Security-Experte Stephan weiter. "So bleibt die Kommunikation konsistent und Fragen werden direkt an zentraler Stelle beantwortet, ohne dass redundante E-Mails verschickt werden müssen."

Vorbereitung ist der Schlüssel

Ein gut durchdachter Incident Response Plan ist mehr als nur eine Sammlung von Notfallmaßnahmen. Er ist ein essenzielles Instrument, das dabei hilft, in Krisenzeiten den Überblick zu behalten, Fehler zu vermeiden und schnell zu reagieren. TOPdesk unterstützt Organisationen dabei, ihre Umgebung optimal für Incident Management zu gestalten und Vorfälle effizient zu bewältigen. Wer frühzeitig die richtigen Vorkehrungen trifft, ist im Ernstfall klar im Vorteil.

Sind Sie bereit, Ihre Cybersicherheit auf das nächste Level zu heben? Mehr Informationen zum Thema und eine Vorlage zur Erstellung Ihres eigenen Incident Response Plans finden Sie im TOPdesk Blog unter: https://www.topdesk.com/de/blog/krisenmanagement-incident-response-plan/.

Pressekontakt:

TOPdesk Deutschland GmbH
Thorsten Becker
t.becker@topdesk.de
0631 624 000
www.topdesk.de

Medieninhalte

Incident Response Plan / Weiterer Text über ots und www.presseportal.de/nr/121184 / Die Verwendung dieses Bildes für redaktionelle Zwecke ist unter Beachtung aller mitgeteilten Nutzungsbedingungen zulässig und dann auch honorarfrei. Veröffentlichung ausschließlich mit Bildrechte-Hinweis.