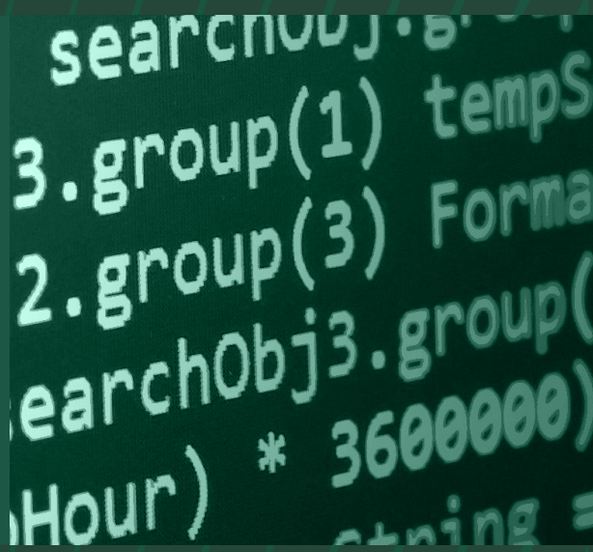
DELL Technologies

5 Empfehlungen für das Überstehen eines Ransomwareangriffs



1 Halten Sie einen umfassenden Incident-Reaktion splan aufrecht

Auf die Minimierung der Auswirkungen eines Angriffs fokussieren

Regelmäßig Übungen, Tests und Updates durchführen

Ein Incident-Reaktionsteam im Voraus zusammenstellen

Cyberversicherung als Teil Ihrer allgemeinen Ausfallsicherheitsstrat-egie erwägen

Pläne für die Zusammenarbeit mit Strafverfolgungsbe-hörden einschließen

2 Erarbeiten Sie eine klare Kommunikations-strategie

Kommunikationsvorla-gen im Voraus erstellen

Zeitnahe und klare Kommunikation innerhalb des Unternehmens sicherstellen

Auf externe Kommunikation vorbereitet sein, falls zutreffend

Geltende Meldevorschriften einhalten

3 Stellen Sie eine robuste Data Protection sicher

Kritische Daten in einem isolierten, unveränderlichen Daten-Vault mit Air Gap schützen

Recovery nach Service/Infrastruktur priorisieren

Wiederherstellbarkeit einüben

Funktionen wie einen Reinraum mit Ihrer Recovery Time Objective (RTO) koppeln

Integrität wiederherstellbarer Daten sicherstellen

4 Gehen Sie nicht von einer sofortigen Rückkehr zur Normalität aus

Lösegeldzahlung als letzten Ausweg betrachten

Einhaltung von gesetzlichen und behördlichen Auflagen sicherstellen, bevor Sie zahlen

Keine Sicherheit, dass HackerInnen Ihre Daten zurückgeben, selbst wenn Sie Lösegeld zahlen

5 Legen Sie den Schwerpunkt auf Schulung und Weiterbildung

Angriffssimulationen durchführen

Sicherheitshygiene-praktiken von MitarbeiterInnen überwachen und testen

Tools wie Phishingtests und E-Mail-Sicherheitsschu-lungen verwenden

Die Frage lautet nicht mehr, „ob“, sondern „wann“.

Unternehmen müssen bei ihrer Planung davon ausgehen, dass ein Angriff trotz bester Abwehrmaßnahmen unvermeidlich ist. Die Dell Subject Matter Experts Jim Shook, Global Director of Cybersecurity and Compliance Practice, und Steven Granat, Principal Consultant, Cybersecurity Solutions and Strategic Partnerships, haben sich mit Brian White, Senior Consultant, Product Marketing for Dell Data Protection, zusammengesetzt, um zu besprechen, was im Katastrophenfall zu tun ist.

> „Sie müssen die richtigen MitarbeiterInnen hinzuziehen, Abläufe einüben und Maßnahmen simulieren, damit bei einem Angriff alle sofort wissen, was zu tun ist.“
>
> ***Steven Granat**, Principal Consultant, Cybersecurity Solutions and Strategic Partnerships, Dell Technologies*

Halten Sie einen umfassenden Incident-Reaktionsplan aufrecht

Wenn es zu einem Angriff kommt, müssen alle wichtigen StakeholderInnen – d. h. so ziemlich alle Personen im Unternehmen und auch Dritte wie Lieferanten – wissen, was zu tun ist. Ein schriftlicher Incident-Reaktionsplan sollte eine klare Abfolge von Maßnahmen vorgeben, rät Shook. Ein umfassender Plan beinhaltet die technologischen sowie die prozess- und kommunikationsbezogenen Schritte von sofortigen Maßnahmen bis hin zur Recovery. Stellen Sie sicher, dass Sie den Plan auch auf Papier ausgedruckt aufbewahren, da digitale Kommunikationsmittel möglicherweise nicht funktionieren. „Sie brauchen einen Plan, den Sie buchstäblich einfach aus dem Regal ziehen können“, so Granat.

Erarbeiten Sie eine klare Kommunikationsstrategie

Die meisten Unternehmen müssen mit wichtigen StakeholderInnen kommunizieren und in vielen Fällen behördliche Auflagen einhalten. Erstellen Sie verschiedene Vorlagen für die interne und externe Kommunikation mit systematischen Anweisungen, wer in welcher Reihenfolge und wann benachrichtigt werden muss. Rechnen Sie mit einem Ausfall von Telefon- und E-Mail-Systemen.

Implementieren Sie eine robuste Data-Protection-Strategie

Ein wichtiges Ziel beim Überstehen eines Ransomwareangriffs ist eine möglichst mühelose Wiederherstellung der Daten und des Betriebs sowie die Vermeidung von Lösegeldzahlungen. Eine robuste Data-Protection-Strategie ist ein wichtiger Bestandteil, um diese Ziele zu erreichen, muss aber sowohl die Technologie als auch Prozesse umfassen. „Verwenden Sie unveränderliche Daten- und Cyber-Vaults, um genügend Daten zu speichern, denen Sie vertrauen oder die Sie zumindest als Validierungspunkte für die Wiederherstellung von Systemen nutzen können“, rät Shook. Der erste Schritt besteht darin, sicherzustellen, dass die Daten geschützt sind. Außerdem benötigen Sie die MitarbeiterInnen und Prozesse, mit denen die Daten wiederhergestellt werden können. Externe ExpertInnen können helfen, sollten aber bereits in der Planungsphase hinzugezogen werden.

Gehen Sie nicht von einer sofortigen Rückkehr zur Normalität aus – selbst wenn Sie Lösegeld zahlen

Eine Lösegeldzahlung, die nur als letzter Ausweg in Betracht gezogen werden sollte, garantiert nicht, dass der Betrieb sofort wiederhergestellt wird. Denken Sie daran, dass Sie mit Kriminellen verhandeln. Selbst wenn Sie die Entschlüsselungsschlüssel erhalten, benötigen Sie eine Strategie für neu wiederhergestellte Daten. Zunächst müssen Sie die entschlüsselten Daten testen und alle Systeme methodisch neu aufbauen. Die wiederholte sorgfältige Berücksichtigung von Was-wäre-wenn-Ereignissen, bevor es überhaupt zu einem Angriff kommt, trägt wesentlich dazu bei, Ausfallsicherheit zu erreichen. „Das Verstehen der verschiedenen Anwendungen und Abhängigkeiten in Ihrer technischen Infrastruktur ist entscheidend für eine effiziente Rückkehr zum stabilen Zustand. Haben Sie eine brauchbare Recovery-Quelle und ein wiederherstellbares Ziel? Verfügen Sie über Daten, die nicht kompromittiert wurden? Dies sind einige wichtige Überlegungen, die Sie anstellen sollten“, erklärt Granat.

In der Recovery-Phase müssen Sie außerdem sicherstellen, dass AngreiferInnen Ihre Systeme tatsächlich verlassen haben. „Sie müssen sicherstellen, dass das Feuer in Ihrem Haus erloschen ist. Sie müssen außerdem herausfinden, was das Feuer überhaupt ausgelöst hat, denn ohne diese zwei wichtigen Informationen sind Sie weiter anfällig für zukünftige Angriffe“, so Shook.

Schulungen und praktische Übungen sind entscheidend

Ein wichtiger Bestandteil der Ausfallsicherheit bei Cyberangriffen sind umfassende Schulungen, die von der Sicherstellung einer strengen Cybersicherheitshygiene bei den MitarbeiterInnen bis hin zum routinemäßigen Üben des Recovery-Plans reichen. „Sie müssen die richtigen MitarbeiterInnen hinzuziehen, Abläufe einüben und Maßnahmen simulieren, damit bei einem Angriff alle sofort wissen, was zu tun ist“, sagt Shook.

Ransomwareangriffe sind in der heutigen Bedrohungslandschaft möglicherweise unvermeidlich. Mit einer guten Planung und Ausführung können Sie jedoch die betrieblichen, finanziellen und rufschädigenden Auswirkungen minimieren. Ziel ist es, so schnell und mühelos wie möglich zur Normalität zurückzukehren.

Erfahren Sie, wie Sie einige der größten Herausforderungen von heute im Bereich der Cybersicherheit bewältigen können: **dell.com/cybersecuritymonth**.

DELL Technologies