REFERENZ ::: Hackerangriff auf ISP Datencenter

Unsere Referenzen - Ihre Garantie

Sie haben noch nie von der birrer.network ag gehört oder gelesen?

Wir führen Arbeiten mehrheitlich für IT Systemhäuser aus.
Als Subunternehmer treten wir somit kaum in Erscheinung.
Endkunden von Kleinst-KMU bis hin zu internationalen Konzernen, vom Netzwerkbetrieb über IT Performance Optimierungen bis hin zur Schadensbehebung nach betriebsschädigenden Hackerangriffen, zählen zu unserem Erfahrungsschatz.
Zudem bewegen wir uns in einem beruflichen Umfeld von höchster Diskretion, was uns von Pomp und medialer Gloria fernhält.

Trotzdem dürfen wir unsere Kompetenzen durch Referenzprojekte anpreisen. Diese geben einen Einblick in unser Schaffen und die Herausforderungen, welche wir meist im Stillen meistern.

Ausgangslage

Der Kunde ist IT Dienstleister und bietet unter anderem Cloud-Lösungen für kaufmännische Unternehmen via Remote Arbeitsplätzen, sowie Kino-Kassensysteme und weitere schweizweit eingesetzte Dienste an. Einige Systeme im Datencenter wurden gehackt. So blieb nur noch, sämtliche Internetverbindungen zu kappen, um die korrumpierten Systeme, zumindest in der Kommunikation nach aussen, zu isolieren.
Nach rund einer Woche Betriebsaufall wurden wir auf Platz gerufen und übernahmen zusammen mit dem IT-Leiter, das Krisenmanagement.
Der Kunde, sowie die Endkunden standen, entsprechend unter hohem Druck.

Herausforderungen

- Erkennen und verstehen wie das Datencenter (Systeme, Netzwerk, etc) physisch und logisch aufgebaut ist.
- Welche Massnahmen wurden bereits unternommen und diese in die (Sofort-)Massnahmen einfliessen lassen.
- Kommunikation nach innen und aussen - fachlich stufengerecht und adressatgerecht.
- Innert kürzester Zeit planen, bauen und laufend bestehende Systeme integrieren des neuen Netzwerksetups inkl. Neukonfiguration Firewall.
- Unterstützend arbeiten, mit einem Top-Team, in deren gewohnten Umgebung, unter höchstem Zeitdruck.

Projekt Zusammenfassung

Kunde
Schweizer Datencenter- und Cloudlösungsanbieter aus dem Raum Bern.

Ausgangslage
Einige Systeme im Datencenter eines Internet Service Providers (ISP) sind gehackt. Der Betreiber trennte das Datencenter vom Internet, was dazu führte, das sämtliche Cloud-Dienste für die Kunden nicht mehr erreichbar waren. Nach rund einer Woche des Ausfalls kontaktierte der Anbieter die birrer.network ag.

Ziel
- Erkennen und isolieren der korrumpierten Systeme.
- Aufbau eines neuen Sicherheitsdispositivs.
- Phasenweise Inbetriebnahme der „sauberen“, produktiven Management- und Kundensysteme.
- Übergang in den regulären Betrieb.

Auftrag
- Führen des Krisenstabs.
- Kommunikation intern und extern koordinieren.
- Technischer Aufbau eines neuen Firewall-Dispositivs.

Resümee

Die Sofortmassnahmen betrafen vor allem kommunikatorische Herausforderungen, um die Kunden nicht zu verlieren. Auch das Erstellen des Projektsplans und die Ressourceneinteilung für den phasenweisen Aufbau des neuen Firewall-Dispositivs, sowie die Reaktivierung produktiver Dienste wurde innert kürzester Zeit nach der 80:20-Regel erstellt.

Innert rund einer Woche konnten die wichtigsten Kundensysteme wieder operativ genutzt werden. Dabei wurden sämtliche Systeme intensiv auf Sicherheitsmängel geprüft, bevor sie aus der Isolation wieder in das Produktive überführt wurden. Im Anschluss wurden die infizierten Systeme aus der Isolation entfernt und neu gebaut. Am Ende wurden die Konfigurationen aller System (Firewalls, Switche, Router, Windows- und Linuxserver) nochmals überprüft und verfeinert.

Der Auftrag wurde gem. Kundenanforderung erfolgreich ausgeführt.