Under Ransom

By

ARCTIC WOLF

END CYBER RISK

HINTERGRUND DES UNTERNEHMENS: SIDEKICKS – Folie 3

SideKicks – ein aufstrebendes Schuhunternehmen – hat mit seinem Online-Vertriebsmodell, das sich auf nachhaltige Materialien und Bauprozesse konzentriert, Erfolge erzielt.

17% - Durchschnittliche 3-Jahres-Wachstumsrate

7 Mio. $ - Umsatz im letzten Quartal

$80k – Ungefährer Tagesumsatz

In den letzten Jahren hat Sidekicks sein Vertriebsmodell auf stationäre Geschäfte in wichtigen globalen Märkten ausgeweitet.

38 Filialen in Grossbritannien, Frankreich, Deutschland, der Schweiz und Österreich

Die Produktion für die Schuhe erfolgt in Übersee in Fabriken in Südkorea und China. Es gibt auch Bekleidung, die jedoch nur einen nominellen Teil des Geschäfts ausmacht.

In einem kalkulierten Schritt, der darauf abzielt, Abfall und Lagerhaltungskosten zu reduzieren, setzt Sidekicks ein Just-In-Time-Bestandsverwaltungssystem ein. Alle Bestellungen und Verkäufe werden in der Zentrale über die Inventarsoftware in Echtzeit verfolgt. Die Produktionsstätten haben auch Zugriff auf das Bestandssystem, und wenn die Mindestschwellen erreicht sind, wird der Ersatzbestand automatisch zu den Bestellungen hinzugefügt und an ein Distributionszentrum in der Nähe des Hauptsitzes geliefert.

Sidekicks verfügt über ein kleines, aber sehr effizientes IT/Sicherheitsteam. Alle Mitarbeiter in der Zentrale, die einen Laptop benötigen, erhalten denselben Laptop, der von der IT-Abteilung vor ihrem ersten Arbeitstag konfiguriert wurde. Alle Berechtigungen werden genau überprüft und Benutzern basierend auf einer Mindestzugriffsrichtlinie zugewiesen. Die gesamte Software ist vorab genehmigt. Es gibt einige Softwareprogramme, die für den Vertrieb zu Berichtszwecken einzigartig sind. Die gesamte Software wird aus der Ferne bereitgestellt.

Sidekicks hat grundlegende IT-Technologie, einschliesslich AV, Perimeter-Firewalls und VPN implementiert.

CHARAKTERE: Folien 6-8

(* Charaktere können bei Bedarf von derselben Person gespielt werden)

Erzähler

IT-Helpdesk *

IT-Leiter

Betriebsleiter

CIO

Anwalt für Datenschutz

Versicherungsvertreter

**

CEO

CFO

Lagerleiter ***

Direktor für E-Commerce **

Leiterin der Personalabteilung *

Vizepräsident für Marketing ***

Leiter des Incident-Response-Teams

AKT 1 – Entdeckung – Folie 9

ERZÄHLER

Es ist Montagmorgen in China – Sonntagabend in Zürich. Der Lagerleiter ist nach dem freien Wochenende früh gekommen und loggt sich in das Bestandssystem ein.

LAGERLEITER

Das ist merkwürdig. Wir haben über das Wochenende keine Bestellungen für SideKicks erhalten. Ich sehe keine Änderungen am Bestand und es gab keine Produktionsläufe. Ich möchte Sidekicks über das Wochenende nicht belästigen, aber ich melde mich morgen, wenn wir immer noch keine neuen Bestellungen sehen.

ERZÄHLER

Acht Stunden später. Das Team in Zürich kommt am Montagmorgen um 8 Uhr im Büro an. Der Lagerleiter hat eine E-Mail an die IT-Abteilung geschickt, in der es um den Mangel an Bestellungen am Wochenende geht.

DIREKTOR FÜR E-COMMERCE

Was passiert? Warum kann ich meine Verkaufsberichte nicht öffnen? Alle meine Symbole sehen unterschiedlich aus, und ich brauche diese Tabellenkalkulationen, um mich auf die Besprechung am Montagmorgen vorzubereiten. Ich werde die IT-Abteilung anrufen müssen.

IT-HELPDESK

Guten Morgen. IT-Helpdesk.

DIREKTOR FÜR E-COMMERCE

Hallo – ich brauche Hilfe. Ich kann meine Verkaufsberichte nicht öffnen und brauche sie für meine morgendliche Besprechung.

IT-HELPDESK

Was siehst du auf dem Bildschirm?

DIREKTOR FÜR E-COMMERCE

Alle meine Desktop-Symbole sehen anders aus, und es sieht so aus, als ob meine Tracking-Tabelle völlig durcheinander ist. Die Datei hat nun die Endung ".Royal".

IT-HELPDESK

Das klingt nach Ransomware. Schalten Sie Ihren Computer aus und rufen Sie Ihr Team an. Sagen Sie ihnen, dass sie die VPN-Verbindung trennen und ihre Computer vorerst ausschalten sollen.

DIREKTOR FÜR E-COMMERCE

Was?!?! Es ist Montagmorgen. Ich kann nicht einfach aufhören zu arbeiten – ich muss die Verkaufszahlen der letzten Woche melden.

IT-HELPDESK

Leider ist das vorerst die einzige Option. Wenn es sich um Ransomware handelt, müssen wir sicher sein, dass sie sich nicht weiter ausbreitet. Ich werde dieses Problem jetzt eskalieren.

ERZÄHLER

Der Helpdesk-Mitarbeiter legt auf und geht direkt zum IT-Manager, um das Problem zu melden.

IT-HELPDESK

Hey - ich habe gerade einen Anruf vom E-Commerce-Team erhalten. Es sieht so aus, als ob das System des Direktors von Ransomware betroffen ist.

IT-LEITER

Oh nein! Ich habe gerade einen Bericht von der Produktionsstätte in China erhalten, und sie haben am Wochenende null Bestellungen erhalten. Ich frage mich, ob die beiden Ereignisse zusammenhängen??

IT-HELPDESK

Ich hasse

Montage.

IT-LEITER

Wir werden das weiter untersuchen müssen. Können Sie das Inventarsystem überprüfen?

IT-HELPDESK

Ich kann es versuchen. Ich denke, der einzige Zugang, den ich habe, ist über die Weboberfläche.

IT-LEITER

OK – während Sie das tun, werde ich herausfinden, wer für Operations auf Abruf ist.

ERZÄHLER

Ein paar Minuten vergehen.

IT-HELPDESK

Ja - es sieht so aus, als ob das Inventarsystem auch betroffen ist. Die

Benutzeroberfläche wird nicht einmal geladen.

IT-LEITER

Davor hatte ich Angst. Ich rufe jetzt Operations an.

BETRIEBSLEITER

Hallo. Wie kann ich dir

helfen?

IT-LEITER

Hey, hier ist die IT. Wir haben ein paar Anrufe erhalten, und es sieht so aus, als ob wir von Ransomware betroffen sein könnten. Wir sind uns nicht sicher, wie weit verbreitet die Dinge sind, aber es scheint sich sowohl auf die Endbenutzer als auch auf das Inventarsystem auszuwirken.

BETRIEBSLEITER

IST DAS DEIN ERNST? Wann hat das angefangen?

IT-LEITER

Nun, wir sind uns nicht ganz sicher, aber es sieht so aus, als ob es irgendwann an diesem Wochenende passieren wird. Seit Freitagabend sind keine neuen Bestellungen mehr eingegangen. Der Helpdesk bestätigte, dass er nicht auf die Inventar-Webschnittstelle zugreifen kann.

BETRIEBSLEITER :

Igitt. Lassen Sie mich einen

genaueren Blick darauf

werfen.

Ja. Das ist ein Problem. Wenn ich eine RDP-Verbindung zu diesem Server trage, scheinen die meisten Dateien verschlüsselt zu sein, mit Ausnahme einer Lösegeldforderung.

IT-LEITER

Davor hatte ich Angst. Wir müssen bewerten, wie weit verbreitet dies ist.

BETRIEBSLEITER

Einverstanden. Möglicherweise müssen wir auch erklären, warum dies durch unsere AV-Lösung nicht verhindert wurde?

IT-LEITER

Ich hatte noch nicht einmal die Gelegenheit, diese Protokolle zu untersuchen. Aber wenn es nicht blockiert wurde, gibt es nichts in den AV-Protokollen. Es ist nicht so, dass wir eine 24x7-Ereignisüberwachung haben.

BETRIEBSLEITER

Ich denke, das ist eine Diskussion für ein anderes Mal. Im Moment haben wir keine andere Wahl, da sich dies direkt auf das Geschäft auswirkt. Wir werden einen internen Sicherheitsvorfall eröffnen und die Führungskräfte benachrichtigen müssen.

ACT 1 Diskussion – Siehe PPT-Folie 12

AKT 2 – Der Impact – Folie 13

ERZÄHLER

Der Operations Manager initiiert das offizielle Incident-Protokoll. Innerhalb einer Stunde sind
IT, Operations, CEO, CIO, CFO und Datenschutzanwalt alle am Telefon. Es ist jetzt 9 Uhr.

BETRIEBSLEITER

Heute Morgen erhielten wir zwei verschiedene Meldungen, die darauf hindeuten, dass wir Opfer eines Ransomware-Angriffs sind. Das Lager in China hat am Wochenende keine Bestellungen erhalten und bestimmte Personen können nicht auf ihre Laptops zugreifen.

CIO

Besteht die Möglichkeit, dass sich die Ransomware immer noch im Netzwerk ausbreitet?

IT-LEITER

Nein. Wir haben alle betroffenen Systeme eingedämmt, während wir sie untersuchen und beheben. Als Vorsichtsmassnahme haben wir auch die RDP- und VPN-Funktionen deaktiviert, um jegliches Risiko im Zusammenhang mit Remote-Mitarbeitern auszuschliessen.

CIO

Warum kommen keine Aufträge in der Fertigung an?

BETRIEBSLEITER

Es scheint, dass das Inventarsystem komplett ausgefallen ist. Wir arbeiten mit dem Team zusammen, um zu verstehen, wie wir es wiederherstellen können. In der Zwischenzeit können wir Online-Bestellungen nicht bearbeiten. Wir hoffen, bald ein Update zu haben.

CFO

Wie hoch ist die Lösegeldzahlung? Wir verlieren jede Stunde Geld, in der wir keine Schuhe verkaufen können. Ganz zu schweigen davon, dass wir einige langjährige Kunden verlieren könnten, wenn bekannt wird, dass wir angegriffen wurden.

BETRIEBSLEITER

Diese Zahl haben wir noch nicht. Die Lösegeldforderung weist darauf hin, dass wir einen Entschlüsselungsschlüssel erhalten, sobald wir das Lösegeld bezahlt haben. Aber zuerst müssen wir den Angreifer kontaktieren, um die tatsächliche Nachfragezahl zu erhalten. (Lösegeldforderung als Anhang A enthalten)

CIO

Wie schnell können wir das Inventarsystem wieder in Gang bringen?

IT-LEITER

Wir versuchen immer noch, das herauszufinden.
Wir haben Backups bei einem Drittanbieter, aber niemand ist mit dem Wiederherstellungsprozess vertraut. Der Mann, dem dieses Projekt gehörte, ging letztes Jahr in den Ruhestand, und wir suchen nach allen Unterlagen, die er

hatte. Ich werde mich in 30 Minuten mit einem Status zurückmelden.

ANWALT FÜR DATENSCHUTZ

Es könnte an der Zeit sein, den Versicherungsanbieter zu beauftragen, falls Sie einen Anspruch geltend machen müssen.

ERZÄHLER

Während der Anruf aktiv bleibt, machen sie eine 30-minütige Pause, um weitere Informationen zu sammeln. Es ist jetzt 9:45 Uhr.

BETRIEBSLEITER

OK – hier ist das Update. Während wir noch ermitteln, scheint es sich um einen gezielten Angriff zu handeln. Da die betroffenen Systeme auf kritische Vertriebs- und Fulfillment-Systeme beschränkt sind, scheint der Angreifer einen Plan zu haben. Wir haben die Server verloren, auf denen unser Inventarsystem, die Auftragsabwicklung und die Verkaufssoftware laufen. Sie nahmen auch die Dateiserver und etwa ein Dutzend PCs offline, die über Buchhaltungssoftware, Auftragsabwicklungs- und Bestandsverfolgungssoftware verfügen. Darüber hinaus luden die POS-Systeme im Rahmen ihrer täglichen Synchronisierung über Nacht beschädigte Dateien herunter. Jetzt sind also alle Filialen nicht mehr erreichbar.

CFO

Dieser Angriff hat uns also völlig unfähig gemacht, Geld zu verdienen.

CIO

Können wir nicht einfach aus Backups wiederherstellen?

IT-LEITER

Für die Kassensysteme der Filialen haben wir tägliche Backups, die 7 Tage zurückreichen. Es sieht jedoch so aus, als ob die Dateien vom Samstag und Sonntag Müll sind. Wir müssen die Dateien vom Freitag wiederherstellen.

HAUPTGESCHÄFTSFÜHRER

Die Geschäfte im Deutschland öffnen in weniger als einer Stunde. Wie lange wird es dauern, bis die Kassensysteme wieder in Betrieb sind?

IT-LEITER

Wir müssen die Content-Server wiederherstellen und dann die Remote-POS-Systeme auslösen, um einen ungeplanten Download durchzuführen. Es kann ein paar Stunden dauern.

CIO

Wie sieht es mit E-Commerce aus? Werden Bestellungen über die Website abgewickelt?

BETRIEBSLEITER

Ja und nein. Wir haben bestätigt, dass die Website online ist. Die Website selbst scheint von dem Angriff nicht betroffen oder kompromittiert zu sein. Ab sofort funktioniert es und nimmt Bestellungen entgegen. Diese Bestellungen werden jedoch aufgrund der Backend-Probleme nicht bearbeitet.

CFO

Das bedeutet, dass Kreditkarten nicht belastet werden, weil die Bestellungen nicht ausgeführt werden.

HAUPTGESCHÄFTSFÜHRER

Das wird immer schlimmer.

CFO

Ich werde unsere Versicherung anrufen, um ihren Rat zu erhalten.

CIO

Okay. Sobald die Systeme also wiederhergestellt sind, kann der Rückstau an Online-Bestellungen abgearbeitet werden.
Es klingt, als ob das grösste Problem für den E-Commerce darin besteht, dass die Leute ihre Schuhe nicht rechtzeitig erhalten.

HAUPTGESCHÄFTSFÜHRER

Nun, das ist fast eine gute Nachricht.

Was machen wir mit den Geschäften? Wie können sie Schuhe ohne ihre POS-Systeme verkaufen?

BETRIEBSLEITER

Hmm... Nun, sie können keine Sonderbestellungen bearbeiten, weil das Inventarsystem ausgefallen ist. Darüber hinaus kann die Kreditkartenverarbeitung auf den POS-Systemen im aktuellen Zustand nicht durchgeführt werden. Sie könnten potenziell In-Store-Inventar verkaufen, aber nur über Bargeldtransaktionen.

HAUPTGESCHÄFTSFÜHRER

OKAY. Lassen Sie mich das klarstellen. Entweder öffnen wir die Läden nicht ODER wir öffnen, und sie können nur Bargeldtransaktionen für lokales Inventar abwickeln?

IT-LEITER

Eine andere mögliche Option wäre, dass Kunden Bestellungen über die Website von ihren Telefonen aus aufgeben können?? Das würde den Rückstand vergrössern, aber zumindest könnten sie Aufträge abgeben.

HAUPTGESCHÄFTSFÜHRER

Ich glaube nicht, dass viele Leute unsere Schuhe mit Bargeld kaufen, aber das Öffnen ist wahrscheinlich immer noch die beste Wahl. Ich hoffe, dass wir dieses Chaos bald gelöst haben.

BETRIEBSLEITER

Ich werde einen Prozess aufschreiben, um die Einzelhandelsgeschäfte zu öffnen. Wir können jeden Manager anweisen, Bargeld von der Bank abzuheben und die Geschäfte mit eingeschränkter Funktionalität zu öffnen.

CFO

Ich habe gerade mit unserer Versicherung gesprochen. Angesichts der Schwere des Problems empfahlen sie uns, ein Incident-Response-Team zu beauftragen. Da wir mit keinem einen Retainer abgeschlossen haben, haben sie uns einige Namen gegeben.

HAUPTGESCHÄFTSFÜHRER

Ist ein Incident Response Team wirklich notwendig?

CIO

Ich denke schon. Wir sind einfach überfordert.
Hoffentlich kann uns ein Incident-Response-Team helfen, mit dem Angreifer zu kommunizieren und den Lösegeldforderungen auf den Grund zu gehen.

CFO

Wir haben einen Scoping-Anruf in einer Stunde geplant, und sie senden den Papierkram für den Fall, dass wir uns entscheiden, es offiziell zu machen.

ACT 2 Diskussion – Folien 11-12

AKT 3 – Die Response – Folie 13

ERZÄHLER

Zu diesem Zeitpunkt ist es fast Mittag. Mit einem provisorischen Plan geht das Team zu einem Anruf mit externen Parteien über, einschliesslich der Versicherungsgesellschaft und der neu eingestellten Incident-Response-Firma. Der Operations Manager hat sie über den aktuellen Status informiert, einschliesslich der Anzahl der betroffenen Systeme, des Status der Backups und der Eindämmungsmassnahmen.

HAUPTGESCHÄFTSFÜHRER

Was ist das Neueste über die Geschäftstätigkeit?

CFO

Wir laufen Gefahr, jeden Tag, an dem wir keine neuen Bestellungen bearbeiten können, 80.000 US-Dollar zu verlieren. Es scheint, dass Samstag und Sonntag bereits verloren sind. Mit der Beeinträchtigung unseres Geschäftsbetriebs und den Verzögerungen bei der Herstellung und dem Versand werden wir einen echten Schlag erleiden - ganz zu schweigen davon, wie sich dies negativ auf unseren Ruf im Kundenservice auswirken könnte. Wir sollten in Erwägung ziehen, das Lösegeld zu zahlen. Haben wir schon eine Zahl?

IT-LEITER

Nein. Wir haben den Angreifer nicht kontaktiert.

VERSICHERUNGSVERTRETER

Das ist einer der Gründe, warum wir empfohlen haben, ein IR-Team

einzubeziehen. Sie können helfen, das Lösegeldproblem zu lösen.

LEITER DES INCIDENT-RESPONSE-TEAMS

Ja. Wir können uns an den Angreifer wenden, um seine Forderungen sowie mögliche Behauptungen, dass er Daten exfiltriert hat, besser zu verstehen. Dank der Zusammenarbeit mit Ihrem IT-Manager haben wir die Lösegeldforderung, wir können Ihre verschlüsselten Dateien sehen und wir haben alles, was wir brauchen, um loszulegen.

ANWALT FÜR DATENSCHUTZ

Während Sie diese Informationen durcharbeiten, müssen wir auch Ihre Prioritäten verstehen. Das hört sich so an, als ob Sie sich am meisten Sorgen über Umsatzeinbussen machen? Wenn jedoch immer noch Bestellungen aufgegeben werden, sind vielleicht Erfüllung, Vertrauen und Reputation die grösseren Probleme?

BETRIEBSLEITER

Das ist technisch richtig. Auf der Website gehen immer noch Bestellungen ein, aber sie häufen sich. Nichts wird wirklich erfüllt.

CFO

Auch in unseren Einzelhandelsgeschäften haben wir gravierende Einschränkungen. Sind diese Einnahmeverluste etwas, das wir über unsere Versicherungspolice geltend machen können?

VERSICHERUNGSVERTRETER

Nein - Ihre spezifische Police deckt keine Umsatzeinbussen ab. Es kann jedoch für die

Kosten der Untersuchung und die Anwaltskosten verwendet werden.

CFO

Wie sieht es mit der Lösegeldzahlung aus?

VERSICHERUNGSVERTRETER

Ja – die Versicherungsgelder können bis zu einem bestimmten Betrag zur Zahlung des Lösegelds verwendet werden.

HAUPTGESCHÄFTSFÜHRER

Herrgott. Wir zahlen gutes Geld für diese Versicherung. Man sollte meinen, wir würden tatsächlich verstehen, was abgedeckt ist!

VERSICHERUNGSVERTRETER

Die gute Nachricht ist, dass Sie noch nie eine solches Ereignis hatten. Das bedeutet aber auch, dass die Berichterstattung nicht im Vordergrund steht. Es gibt viele Variablen bei der Cyber-Versicherung und jede Police kann ein wenig anders sein.

HAUPTGESCHÄFTSFÜHRER

Wir können diese Details später durcharbeiten.
Im Moment geht es mir vor allem um die Geschäftslage. Sowohl die E-Commerce- als auch die Store-Experience sind derzeit schrecklich und könnten unserer Marke wirklich langfristig schaden.

LEITER DES INCIDENT-RESPONSE-TEAMS

Verstanden. Sobald wir die Details des Lösegelds verstanden haben, müssen Sie einige schnelle Entscheidungen treffen. Rechtfertigt die Rate des Verlusts oder der Schädigung des Rufs in irgendeiner

Weise die Zahlung des Lösegelds? Ausserdem müssen wir besprechen, wie sich dieser Vorfall auf Ihre Kunden auswirken könnte und was Sie bereit sein sollten, offenzulegen.

BETRIEBSLEITER

Das ist wirklich nur ein IT-Problem. Warum sollten wir dies unseren Kunden offenlegen?

ANWALT FÜR DATENSCHUTZ

Nun, es kommt darauf an. Wenn sie Kundendaten gestohlen haben, ist die Offenlegung von entscheidender Bedeutung. Unabhängig davon sollte jede Kundenkommunikation von unserer Rechtsabteilung genehmigt werden, um den richtigen Detaillierungsgrad und das richtige Timing zu gewährleisten.

So wie es jetzt aussieht, müssen wir möglicherweise in Betracht ziehen, Kunden mit ausstehenden Aufträgen auf die Verzögerungen aufmerksam zu machen.

Könnten Sie die Website auch mit einer Warnung aktualisieren, dass zukünftige Bestellungen längere Ausführungszeiten haben könnten?

BETRIEBSLEITER

Wir sind sicherlich in der Lage, beides zu tun, aber irgendjemand muss die Entscheidungen treffen, wenn es notwendig ist.

HAUPTGESCHÄFTSFÜHRER

Ich würde empfehlen, den VP Marketing zu involvieren. Die haben ein Team, das sich auf die Kunden konzentriert, und sie könnten dazu beitragen, diese Kommunikation zu erleichtern.

ANWALT FÜR DATENSCHUTZ

Eine Sache, die Sie bedenken sollten: Es könnte viel komplizierter werden, wenn der Angreifer behauptet, Kundendaten gestohlen zu haben.

CIO

Nun, wir befinden uns auf unbekanntem Terrain. Welche Überraschungen gibt es noch?

LEITER DES INCIDENT-RESPONSE-TEAMS

Erste Hinweise deuten darauf hin, dass sich dieser Vorfall auf die Verkaufs- und Bestandssysteme konzentrierte. Wenn der Blast Radius grösser ist, besteht auch die Möglichkeit, dass Mitarbeiterinformationen kompromittiert wurden.

HAUPTGESCHÄFTSFÜHRER

In diesem Fall müssen wir auf jeden Fall die Personalabteilung einbeziehen.

ANWALT FÜR DATENSCHUTZ

Auch da können wir helfen. Wenn Mitarbeiterdaten kompromittiert wurden, sollten Sie die interne Kommunikation sowie einen Plan zu ihrem Schutz organisieren.

CFO

Wenn wir diese Umsatzeinbussen nicht in den Griff bekommen, fürchte ich, dass wir aus anderen Gründen die Personalabteilung einbeziehen müssen. Irgendwann könnten Cashflow und Gehaltsabrechnung zum Thema werden.

LEITER DES INCIDENT-RESPONSE-TEAMS

Der beste nächste Schritt besteht darin, die Analyse fortzusetzen. Wir müssen das gesamte Problem verstehen, damit wir auf eine Wiederherstellung und vollständige Wiederherstellung hinarbeiten können.

HAUPTGESCHÄFTSFÜHRER

Was brauchen Sie von uns?

LEITER DES INCIDENT-RESPONSE-TEAMS

Wir erhielten die Lösegeldforderungen und verschlüsselten Dateien. Unser Team arbeitet daran, den Angreifer, seine Motive und Forderungen zu verstehen.

Wir müssen auch forensische Analysen durchführen, die Schwachstelle der Kompromittierung identifizieren und sicherstellen, dass alle Systeme ordnungsgemäss behoben werden.

IT-LEITER

Mein Team kann mit Ihnen daran arbeiten.

LEITER DES INCIDENT-RESPONSE-TEAMS

Wir benötigen Firewall-Protokolle und Antiviren-Protokolle, um die Gesamtauswirkungen zu verstehen. Ausserdem möchten wir alles über Ihre Backup-Verfahren verstehen, einschliesslich Verschlüsselung, Zeitpläne und welche Systeme, wenn überhaupt, nicht regelmässig gesichert werden.

IT-

MANAGER:

Wir sind

dran.

ACT 3 Diskussion – Folie 13

AKT 4 – Die Recovery – Folie 14

ERZÄHLER

Es ist 16 Uhr. Das IT-Team hat die Protokolle zur Überprüfung bereitgestellt, und das IR-Team hat Verhandlungen mit dem Bedrohungsakteur aufgenommen. Der VP of Marketing und der Director of Human Resources haben sich dem Gespräch angeschlossen.

LEITER DES INCIDENT-RESPONSE-TEAMS

Wir haben einige Neuigkeiten aus unserer Untersuchung.
Erstens beträgt die anfängliche Lösegeldforderung eine Million Dollar. Der Angreifer behauptet jedoch nicht, Kunden- oder Mitarbeiterdaten gestohlen zu haben. Wenn das stimmt, basiert die Entscheidung, das Lösegeld zu zahlen, fast ausschliesslich auf der Erfüllung und den Auswirkungen auf den Umsatz.

HAUPTGESCHÄFTSFÜHRER

Wenn sie keine Kundendaten haben, warum sollten wir dann so viel Lösegeld zahlen?

CFO

Bei einer Million Dollar müssten wir 12,5 Tage ausfallen, um es allein mit den Einnahmen zu rechtfertigen.

CIO

Ich gehe wirklich nicht davon aus, dass wir so lange offline bleiben.

CFO

Vielleicht auch nicht. Aber wenn wir erfolgreich ein niedrigeres Lösegeld aushandeln können, wird diese Zeitspanne noch kürzer. Umsatzeinbussen, die auch nur sechs Tage dauern, würden die Zahlung einer halben Million

Dollar rechtfertigen. Ausserdem deckt die Versicherung möglicherweise all das ab. Ich denke, wir sollten in Erwägung ziehen, zu zahlen und das hinter uns zu lassen.

HAUPTGESCHÄFTSFÜHRER

Bevor wir erwägen, einen Antrag auf Zahlung des Lösegelds zu stellen, sollten wir alle möglichen Auswirkungen auf unsere Prämien und die zukünftige Versicherbarkeit verstehen.

CFO

Fairer Punkt.

CIO

Es scheint, dass die Zeit der Recovery der Schlüssel ist. Wie schnell können wir die POS- und Auftragsabwicklungssysteme wiederherstellen?

LEITER DES INCIDENT-RESPONSE-TEAMS

Da haben wir gute Nachrichten. Wir konnten überprüfen, ob die Store-Backups für Freitag in Ordnung sind. Der Prozess zur Wiederherstellung dieser Daten ist im Gange. Wir haben mit den Läden in Deutschland begonnen und bewegen uns nach Frankreich. Wir gehen davon aus, dass diese innerhalb einer Stunde wiederhergestellt werden.

CIO

Grossartig, aber können die Filialen funktionieren, wenn die zentralen Systeme nicht wiederhergestellt werden?

BETRIEBSLEITER

Sobald die POS-Systeme wieder da sind, werden sie in der Lage sein, Bestände in den Filialen mit allen Zahlungsarten zu verkaufen. Alle Änderungen am Bestand oder Sonderbestellungen

werden zwischengespeichert, bis die zentralen Systeme wiederhergestellt sind. Sie funktionieren so, als hätte das Geschäft einen vorübergehenden Internetausfall.

LEITER DES INCIDENT-RESPONSE-TEAMS

Die Wiederherstellung der zentralen Dienste hat sich als etwas komplizierter erwiesen. Die Wiederherstellung des Bestands- und Auftragsabwicklungssystems geht viel langsamer voran, da wir über einen Drittanbieter arbeiten müssen. Wir sind uns nur nicht sicher, wie lange das dauern wird.

BETRIEBSLEITER

Unsere Teams versuchen, das SLA mit dem Drittanbieter und die richtigen Schritte zu verstehen, um sicherzustellen, dass die Wiederherstellung erfolgreich verläuft und keine Aufträge verloren gehen. Wir hoffen, dass die Dinge in den nächsten 1-5 Tagen wieder in Ordnung sind.

CFO

Damit kommen wir der Rechtfertigung der Lösegeldzahlung immer näher.

HAUPTGESCHÄFTSFÜHRER

Wie sehen die Pläne für die Kundenkommunikation aus?

ANWALT FÜR DATENSCHUTZ

Da keine Kundendaten durchgesickert sind, sind wir mit dem Plan des Marketings zufrieden, sich auf den Ruf und die Loyalität der Marke zu konzentrieren.

VIZEPRÄSIDENT FÜR MARKETING

Wir haben drei verschiedene Bemühungen im Gange. Zunächst erhalten Kunden mit aktuellen,

ausstehenden Bestellungen eine E-Mail mit einer Benachrichtigung über die Verzögerung sowie einen Gutscheincode für 20 % Rabatt auf ihre nächste Bestellung.

BETRIEBSLEITER

Wir haben auch ein Banner auf der E-Commerce-Website hinzugefügt, um darauf hinzuweisen, dass neue Bestellungen beeinträchtigt und verzögert werden könnten. Dieses Banner lässt sich leicht entfernen, sobald wir wieder vollständig einsatzbereit sind.

VIZEPRÄSIDENT FÜR MARKETING

Zu diesem Zeitpunkt wird der Rest unserer Kundendatenbank mit einem 10%-Code als Dankeschön für ihr bisheriges Geschäft empfangen. Und schliesslich erhalten Kunden, die heute und morgen im Geschäft einkaufen, einen kostenlosen Hut aus dem vorhandenen Lagerbestand. Wir hoffen, dass dies die Irritationen über die eingeschränkte Funktionalität oder die nicht verfügbaren Grössen und Stile lindern wird.

HAUPTGESCHÄFTSFÜHRER

Das hört sich alles gut an. Es scheint, als gäbe es ein Licht am Ende des Tunnels.

CIO

Gehen wir einen Schritt zurück. Wissen wir, was dieses Chaos ausgelöst hat?

LEITER DES INCIDENT-RESPONSE-TEAMS

Haben wir. Es sieht so aus, als ob der Director of E-Commerce durch Phishing ins Visier genommen wurde. Protokolle zeigen, dass er am Freitagnachmittag auf einen Link geklickt hat, und auf einer gefälschten Microsoft-365-Anmeldeseite sein Passwort eingegeben. Dadurch wurde eine Hintertür zum Netzwerk geschaffen,

die dem Bedrohungsakteur Zugriff und die Möglichkeit gab, sich lateral über das Netzwerk zu bewegen. Sobald er Fuss gefasst hatte, wurde die Ransomware-Payload bereitgestellt und die Dateien verschlüsselt.

CIO

Alles begann mit einer Phishing-E-Mail?!?!

LEITER DES INCIDENT-RESPONSE-TEAMS

Ja. Das ist ziemlich häufig. Ich würde sagen, dass etwa 30 % unserer Ransomware-Untersuchungen auf einen Phishing-Angriff zurückzuführen sind. Die Bösewichte werden immer besser darin, die Angriffe zu tarnen.

ANWALT FÜR DATENSCHUTZ

Haben Sie ein Schulungsprogramm für das Sicherheitsbewusstsein?

PERSONALDIREKTOR

Haben wir. Es handelt sich um ein jährliches Schulungsprogramm, das die Compliance-Anforderungen erfüllt. Wir können diesen Benutzer auf jeden Fall nachverfolgen, zusätzliche Schulungen anbieten und sicherstellen, dass er die Konsequenzen seines Handelns versteht.

VERSICHERUNGSVERTRETER

Sie können sich auch die Gesamteffektivität Ihrer Lösung ansehen. Das könnte bei Ihrer nächsten Versicherungsverlängerung eine Rolle spielen.

PERSONALDIREKTOR

Okay. Wir können das als Massnahme nehmen, nachdem sich der Staub gelegt hat.

HAUPTGESCHÄFTSFÜHRER

Das hört sich so an, als hätten wir noch viel Arbeit vor uns. Aber im Moment müssen wir noch über die Zahlung des Lösegelds entscheiden.

VERSICHERUNGSVERTRETER

Das ist zu 100% Ihre Entscheidung. Ihre Police zahlt bis zu einem bestimmten Betrag.

CFO

Und wenn diese Jungs bereit sind zu verhandeln, können wir einer 100%igen Abdeckung näher kommen.

LEITER DES INCIDENT-RESPONSE-TEAMS

Wir können Ihnen helfen, die Kommunikation mit dem Angreifer zu steuern, wenn Sie die Bezahlung in Erwägung ziehen.

CIO

Basierend auf dem, was ich höre, bin ich zuversichtlich, dass wir die Systeme in den nächsten 4 Tagen wiederherstellen werden. Ich glaube nicht, dass wir dafür zahlen sollten. Wir sollten diesen Tyrannen nicht einfach nachgeben.

VIZEPRÄSIDENT FÜR MARKETING

Ich hoffe, Sie haben Recht. Wir müssen zum Normalbetrieb zurückkehren, bevor wir unsere treuen Kunden verlieren.

CIO

Danach müssen wir ein detailliertes Post-Mortem-Projekt durchführen, um aus diesem Vorfall zu lernen und unsere Prozesse und Pläne für die Zukunft zu verbessern.

LEITER DES INCIDENT-RESPONSE-TEAMS

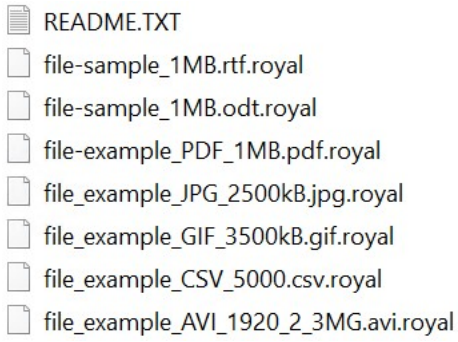
Wir werden mit Ihnen allen an einer vollständigen Nachbereitung arbeiten, um Verbesserungsmöglichkeiten und Möglichkeiten zu identifizieren, wie Sie in Zukunft besser vorbereitet sein können.

DAS ENDE

-

ANHANG A Die Lösegeldforderung und Beispieldateinamen – Folie 11

```
Hello!

    If you are reading this, it means that your system were hit by Royal ransomware.
    Please contact us via : [Royal-operated dark web site]

In the meantime, let us explain this case.It may seem complicated, but it is not!
Most likely what happened was that you decided to save some money on your security infrastructure.
Alas, as a result your critical data was not only encrypted but also copied from your systems on a secure
server.
From there it can be published online.Then anyone on the internet from darknet criminals, ACLU journalists,
Chinese government(different names for the same thing),and even your employees will be able to see your
internal documentation: personal data, HR reviews, internal lawsuits and complains, financial reports,
accounting, intellectual property, and more!

Fortunately we got you covered!

Royal offers you a unique deal. For a modest royalty(got it; got it ? ) for our pentesting services we will not
only provide you with an amazing risk mitigation service, covering you from reputational, legal, financial,
regulatory,
and insurance risks, but will also provide you with a security review for your systems.
To put it simply, your files will be decrypted, your data restored and kept confidential, and your systems will
remain secure.

 Try Royal today and enter the new era of data security!
 We are looking to hearing from you soon!
```



-

ANHANG B Was schief gelaufen ist - Vorschlag

Akt 1

1. Eine frühere Benachrichtigung aus China hätte dazu beitragen können, die Auswirkungen der Ransomware zu minimieren.
2. Wenn Ransomware gemeldet wird, sollte der Helpdesk spezifische Empfehlungen zum Schutz des Netzwerks, aber auch zum Schutz von Artefakten haben. Das Ausschalten eines Geräts wird in der Regel nicht empfohlen.
3. Das Fehlen eines Managed Detection and Response-Dienstes bedeutete, dass sie den Angriff erst bemerkten, als es zu spät war.

Akt 2

4. Das Fehlen eines IR-Retainers kostete wertvolle Zeit bei der Reaktion.
5. Das Fehlen einer Dokumentation über Prozesse und Verfahren führt zu einer Reihe von Rückschlägen.
    a. Fehlende Dokumentation für die Wiederherstellung von Backups von Drittanbietern
    b. Kein dokumentierter Prozess, um ohne POS zu arbeiten

Akt 3

6. Zu spät dran zu sein, bedeutete, dass das IR-Team die Menschen, das Geschäft und ihre Prioritäten während der Reaktion kennenlernen musste.
7. Wenn sie einen Plan für die Arbeit ohne ihr Bestandssystem gehabt hätten, wären sie möglicherweise zu einem manuelleren Prozess übergegangen, um Versandverzögerungen zu minimieren.

-

ANHANG C Das Ergebnis – Folie 15

Bedrohungsgruppen unterhalten Darknet-Shame-Websites, um mit ihren Opfern über Lösegeld zu verhandeln, ihre Namen zu nennen und ihre Daten als Strafe für die Nichtzahlung preiszugeben. Diese Websites dienen als wichtiges Instrument, um Opfer zu bedrohen und Lösegeldzahlungen zu erwirken. Basierend auf dem heutigen Szenario wurde unsere SideKicks-Organisation ins Darknet gestellt, weil sie kein Lösegeld gezahlt hat.