firstcolo

A brand of divaᵉ

ANWENDERBERICHT

Case-Study: Der Weg zu mehr Sicherheit führt in die Cloud

Was sich aus den Ransomware-Angriffen von REvil lernen lässt

Am 7. November 2020 bemerkte der Geschäftsführer eines mittelständischen Bremer Unternehmens, das im An- und Verkauf von Merchandising-Artikeln in Deutschland und Frankreich aktiv ist, einige Unstimmigkeiten im unternehmensinternen Netzwerk. Zum Großteil unterlagen die Serverdaten einer undurchdringbaren Verschlüsselung. Über Nacht startete eine in IT-Kreisen bekannte Gruppe von Hackern unter dem Namen REvil diesen Ransomware-Angriff, der viele Prozesse des Betriebes für mehrere Wochen lahmlegte. Etwa 90 Prozent der Daten verschlüsselten die Hacker und stellten für die Herausgabe des Generalschlüssels, der zur Freigabe jeglicher Dateien befähigt, eine hohe monetäre Forderung von rund 300.000 Euro – ein erschreckendes Szenario, das viele weitere kleine und mittlere Unternehmen (KMU) in Deutschland und weltweit betrifft. In den vergangenen Jahren entwickelte sich ein zunehmend beunruhigender Anstieg an Cyberkriminalität. Lag die Zahl der Fälle in Deutschland 2016 noch bei rund 82.000 Fällen, so verzeichnete das Bundeskriminalamt für das Jahr 2020 bereits über 108.000 Angriffe.[1]

Nacht- und Nebelaktion?

Auch wenn sich diese Attacke scheinbar aus dem Nichts – wie sich im Nachhinein zurückverfolgen ließ – zwischen ein und zwei Uhr nachts ereignete, handelte es sich dabei nicht um eine spontane Aktion der Cyberkriminellen. Vielmehr vermutet der Geschäftsführer, dass sie schon mehrere Wochen zuvor in das System eindringen konnten. Schließlich betraf der Angriff ebenfalls einen bereits seit einem Monat im Homeoffice befindlichen Mitarbeiter des Unternehmens mit Büros in Bremen, Hamburg und Frankreich, der auf seinem Dienstlaptop zeitgleich die Verschlüsselung seiner Daten feststellte und auf keinerlei wichtige Datei zugreifen konnte. Somit zog die Attacke größere Kreise als zunächst angenommen und betraf so gut wie jeden der Mitarbeitenden. Nur durch die Eingabe eines sechsstelligen Hexadezimalcodes ließ sich dieses Problem lösen, ohne dass im Zuge der Attacke wichtige Daten verloren gingen. Mehrere Wochen mussten die Mitarbeitenden die Arbeit mit großen Einschränkungen fortführen, was jedoch so gut es ging gelang, da sich essenzielle Abläufe ebenfalls auf manuellem Wege bewerkstelligen ließen und somit weitestgehend weiterlaufen konnten. Um den wirtschaftlichen Schaden so gering wie möglich zu halten, mussten die

[1] Bundeskriminalamt (BKA): Bundeslagebild Cybercrime 2020

Pressekontakt: Borgmeier Public Relations, Niklas Bädjer/Niklas Römer, Lange Str. 112, 27749 Delmenhorst, Tel: 04221-9345-340/-335, Fax: 04221-9345399, baedjer@borgmeier.de/roemer@borgmeier.de

Verantwortlichen also schnellstmöglich handeln – vor dem Hintergrund der akuten Drucksituation leichter gesagt, als getan.

Good guy, bad guy

Doch was tun, wenn der schlimmste aller Fälle eingetreten ist? Viele IT-Fremde und in diesem Bereich Unerfahrene stellten sich nach gehäuften Meldungen zur aufkeimenden Cyberkriminalität bestimmt schon mehrfach diese Frage. Anders als in vielen Kinofilmen, in denen die Erpresser mit verzerrter Stimme in bedrohlichem Ton das Lösegeld fordern, läuft ein solcher Deal in der Realität weitaus unspektakulärer ab. In diesem Angriffsfall der Gruppierung REvil startete erst nach dem Versuch des Zugriffs auf die gewünschte Datei ein Countdown, der sich auf fünf Tage begrenzte und eine zu bezahlende Forderung enthielt, die sich bei dem betroffenen Unternehmen auf insgesamt 300.000 US-Dollar bezifferte. Summen, die für KMUs eine nicht zu stemmende Last darstellen. Nach Eingang der Forderung konnten die Verantwortlichen in eine Chatkommunikation mit den Kriminellen treten und über das Lösegeld verhandeln. Dabei kristallisierte sich heraus, dass sie es in den zähen mehrtägigen Verhandlungen mit mehreren Tätern auf der Gegenseite zu tun hatten. Auf der einen Seite ein unnachgiebiger, harter Verhandlungspartner und andererseits eine kommunikative, freundliche Person, mit der sich ein Kompromiss schließen ließ. Bei einer weitaus geringeren Summe erzielten sie letztendlich eine Einigung in den Verhandlungen. Da sich kein alternativer Lösungsweg auftat, um die wertvolle Datensammlung von über 20 Jahren erfolgreichem Unternehmertum wiederzuerlangen, beglich die Geschäftsführung den Betrag mit der nicht nachverfolgbaren Kryptowährung Monero.

Kontrolle schlägt Vertrauen

Nach dem Zero-Trust-Prinzip hinterfragte die Führungsetage anschließend jegliche Strukturen und Prozesse, um Sicherheitslücken des Netzwerks möglichst präzise ermitteln zu können. Zur Unterstützung engagierte der Geschäftsführer eine nahe gelegene Bremer IT-Sicherheitsfirma, welche die Situation mit ihrer langjährigen Erfahrung und angesammeltem Know-how in diesem Bereich einschätzen sollte. Dem Rat der Sicherheitsexperten zum totalen Austausch der gesamten Hardware konnte die Geschäftsführung keine Folge leisten, da es die wirtschaftlichen Rahmenbedingungen nicht zuließen. Vonseiten der zuständigen Versicherung kam ebenfalls kein positives Signal zur finanziellen Unterstützung, woraufhin sich das Unternehmen dazu entschied, eine neue IT-Infrastruktur aufzubauen. Auf einer vertrauensvollen Basis engagierte der Betrieb schließlich den Rechenzentrums-Dienstleister firstcolo, der hauseigene Datacenters betreibt und für unterschiedliche Kunden Colocation-,

Pressekontakt: Borgmeier Public Relations, Niklas Bädjer/Niklas Römer, Lange Str. 112, 27749 Delmenhorst, Tel: 04221-9345-340/-335, Fax: 04221-9345399, baedjer@borgmeier.de/roemer@borgmeier.de

sowie Managed Services-Dienstleistungen zur Verfügung stellt. Mitte Dezember 2020 kam es zur ersten Kontaktaufnahme zwischen beiden Parteien. In der weiteren Zusammenarbeit verlagerte der Betrieb seine Datensätze auf das externe Datacenter von firstcolo und verwaltet sie heute aus der Cloud heraus.

Aufstieg in die Cloud

Gerade für mittlere und kleine Unternehmen bietet die Auslagerung von Servern und Daten vielerlei Vorteile. Aus Gründen der Sicherheit ergibt ein Wechsel von der standortbezogenen internen Datenspeicherung zu externen Rechenzentren absolut Sinn, da Dienstleister wie firstcolo die oftmals angemieteten Server rund um die Uhr kontrollieren und somit für eine Rundumüberwachung der Systeme sorgen kann. Verwaltungsaufgaben und Wartungsarbeiten fallen damit nicht mehr in den eigenen Aufgabenbereich, was im Umkehrschluss effektivere Prozesse und finanzielle Einsparungen bewirkt. Denn Hardware, die bei intensiv genutzten Servern gut alle drei bis fünf Jahre ausgetauscht werden muss, stellt für das mietende Unternehmen keinen Kostenfaktor mehr dar. Gerade durch die Corona-Pandemie nehmen flexible Arbeitsmodelle eine immer größere Rolle ein. Egal ob in einem der an verschiedenen Standorten niedergelassenen Büros oder im Homeoffice, die Cloud-Anwendung lässt sich von jedem Standort aus flexibel nutzen. Zudem greifen Angestellte vor allem sicher auf Informationen zu oder nehmen Änderungen am System vor.

Unwissenheit schützt vor Strafe nicht

Um einen Cyberangriff in Zukunft möglichst zu vermeiden, ergriff das Unternehmen neben der Etablierung der neuen IT-Struktur ebenfalls weitere Maßnahmen, um vor allem die Mitarbeitenden – die Kernnutzer des Systems – zu sensibilisieren. In der Regel erlangen Cyberkriminelle, wie vermutlich auch in diesem Fall, durch einen einzelnen User Zugriff auf ein bestehendes System. Genau an diesem Punkt setzten die Verantwortlichen unmittelbar nach der Attacke an, um eine der größten Einfallstellen in einem ansonsten sicheren Netzwerk zu minimieren. Dafür konzipierten sie ein Sicherheitstraining für ihre Angestellten, das sich eigenständig über eine eigens entwickelte Security-Plattform absolvieren lässt. Es enthält umfassende Schulungsunterlagen und einen abschließenden Test, nach dessen erfolgreicher Durchführung jeder User ein Zertifikat ausgehändigt bekommt. Ein großes Thema bleiben dabei oftmals unterschätzte Phishing-Mails, die durch einen Vorwand noch immer viele Nutzerinnen und Nutzer dazu verleiten, auf Fallen von Kriminellen einzugehen und den laufenden Betrieb somit einem großen Risiko aussetzen. Durch die Sicherheitsschulungen gepaart mit der Datenverwahrung in der Cloud durch firstcolo ergibt sich eine IT-Infrastruktur,

Pressekontakt: Borgmeier Public Relations, Niklas Bädjer/Niklas Römer, Lange Str. 112, 27749 Delmenhorst, Tel: 04221-9345-340/-335, Fax: 04221-9345399, baedjer@borgmeier.de/roemer@borgmeier.de

die den Cyberkriminellen in Zukunft beinahe keine Zugangsmöglichkeit bietet. Weiteren Angriffen kann somit proaktiv vorgebeugt werden und das Ergebnis ist ein risikofreier Betrieb der unternehmenskritischen IT.

Weitere Informationen über firstcolo unter first-colo.net.

firstcolo

Als Betreiber von Rechenzentren in Deutschland stellt firstcolo mit Sitz in Frankfurt am Main seinen Kunden das höchste Maß an Servicequalität zur Verfügung. Das Dienstleistungsspektrum von firstcolo umfasst neben klassischer Colocation und der Vermietung von Serversystemen ebenfalls Storage-on-Demand-Lösungen, Backuplösungen und Cloud-Services. firstcolo ist Teil der diva-e Gruppe, die als führender Transactional Experience Partner in Deutschland über 20 Jahre an Branchenexpertise in der digitalen Welt verfügt. Rund 800 Mitarbeiter der diva-e Gruppe kümmern sich in 13 Offices an 8 verschiedenen Standorten um die Anliegen des breitgefächerten Kundenstammes, der einen großen Pool an Branchen aus Technik, Handel und Heathcare umfasst. Darunter fallen neben großen und bekannten Unternehmen wie dem FC Bayern München, Siemens, Mister Spex, Audi oder Sky viele weitere namenhafte Kunden.

Pressekontakt: Borgmeier Public Relations, Niklas Bädjer/Niklas Römer, Lange Str. 112, 27749 Delmenhorst, Tel: 04221-9345-340/-335, Fax: 04221-9345399, baedjer@borgmeier.de/roemer@borgmeier.de