DXC.technology

5 Lektionen, die wir aus dem Ransomware-Angriff auf unser Unternehmen gelernt haben

Von Mark Hughes, Senior Vice President, DXC Technology

> Die Zeit ist bei einem Ransomware-Angriff entscheidend, da eine der schwerwiegendsten Auswirkungen die Ausfallzeit ist.

Es ist schon vielfach berichtet worden, dass die Anzahl der Ransomware-Angriffe zunimmt. Diese Angriffe können gravierende Konsequenzen haben, die sich auf alle Bereiche eines Unternehmens auswirken, darunter Kunden und Betriebsabläufe, die Marke und sogar der Vorstand.

Im Rahmen meiner Tätigkeit bei DXC Technology bin ich für unseren Geschäftsbereich Sicherheit verantwortlich und habe häufig mit Angriffen auf unsere Kunden zu tun. Aber am Samstag, den 4. Juli 2020, als ich gerade aus dem Auto stieg, um in meinen Urlaub mit der Familie zu starten, wurde unser Unternehmen zum Ziel eines Ransomware-Angriffs.

Von dem Angriff war Xchanging betroffen, ein Tochterunternehmen im Vereinigten Königreich, das durch Technologie unterstützte Geschäftsservices für die Versicherungsbranche bereitstellt. Der Angreifer sendete ein häufig verwendetes Bild einer beliebten Zeichentrickfigur mit obszönem Handzeichen zusammen mit der folgenden Nachricht: „Wir haben Ihre Daten. Ihre Dateien wurden verschlüsselt. Wenn Sie verhandeln möchten, können wir uns über ein sicheres Tool oder eine sichere Chat-Sitzung unterhalten.“

Zwar ist das vom Unternehmen Xchanging verwendete Netzwerk vollständig von der viel umfangreicheren IT-Umgebung von DXC getrennt. Dennoch waren wir besorgt, dass der Vorfall sich auf den Geschäftsbetrieb der Kunden von Xchanging auswirken könnte, wenn die Versicherungsbüros in London am Montag öffneten.

Die Zeit ist bei einem Ransomware-Angriff entscheidend, da eine der schwerwiegendsten Auswirkungen die Ausfallzeit ist. Gemäß Emsisoft legt ein durchschnittlicher Angriff die kritischen Systeme 16 Tage lang lahm. Emsisoft prognostiziert, dass die Ransomware-Kosten im Jahr 2020 weltweit insgesamt 170 Milliarden $ betragen könnten.

Bei dem Angriff auf Xchanging war es dem Hacker erst zwei Tage zuvor gelungen, erstmals auf die Systeme zuzugreifen. Es wurde nur auf eine Handvoll Systeme zugegriffen, und wir konnten die Bedrohung schnell isolieren und neutralisieren. Es wurden keine Daten gestohlen, und wir haben das Lösegeld nicht bezahlt. Wir haben sofort unsere Kunden und die Behörden informiert. Am Sonntag, den 5. Juli, haben wir die betroffene Umgebung

bereinigt und wiederhergestellt. Am Montagmorgen war Xchanging für die Verarbeitung von Versicherungspolicen bereit.

Tipps für mehr Sicherheit

Die Ermittlungen der Kriminalpolizei dauern an und wir nehmen jede Gelegenheit wahr, unsere Kontrollinstrumente und Prozeduren zu überprüfen. Fast alles hat funktioniert wie geplant. Das ist jedoch leider in vielen Unternehmen nicht der Fall.

Wir haben analysiert, was gut lief und was nicht, und was wir besser machen können.

Die folgenden fünf wichtigen Erkenntnisse haben wir gewonnen:

Schützen Sie Ihre Infrastruktur. Konzentrieren Sie sich auf grundlegende Hygiene beim Software-Patching und stellen Sie sicher, dass für alle Netzwerke und Firewalls für Unternehmen geeignete Sicherheits-Tools vorhanden sind, die böswilliges Verhalten erkennen. Die Angreifer haben zu Anfang ein öffentlich verfügbares Tool für Sicherheitstests verwendet, das als „Grayware“ eingestuft wird. Grayware ist an sich keine Schadsoftware, wurde aber in diesem Fall verwendet, um eine Hintertür für den Zugriff auf Microsoft Windows zu erstellen und eine neue Variante einer Verschlüsselungs-Malware zu implementieren. Zwar konnten wir den Angriff nicht verhindern. Wir wurden jedoch darüber informiert, dass etwas nicht stimmte, und konnten schnell erkennen, an welcher Stelle das Netzwerk kompromittiert war, als der Angriff lief.

Die Behörden raten dringend von der Lösegeldzahlung ab. In den USA und im Vereinigten Königreich gibt es sogar Bestrebungen, Strafen für die Zahlung von Lösegeld einzuführen.

Beziehen Sie von Anfang an das obere Management ein. Unser globales Krisenteam ist zusammengekommen, um die Situation zu analysieren. Das war für uns sehr wichtig, da die einbezogenen Führungskräfte sehr schnell kritische Entscheidungen treffen konnten. Beispielsweise mussten wir den Remote-Zugriff deaktivieren. Also habe ich die Entscheidung getroffen, sämtliche Verbindungen zu den Systemen von Xchanging zu trennen. Dies klingt zunächst sehr einfach, erforderte jedoch sofortige Aktionen durch unsere IT-Teams im Vereinigten Königreich und in Indien. Da die Führungskräfte dieser Teams eingebunden waren, konnte die Trennung schnell und effizient erfolgen. Während der gesamten Dauer der Krise waren Mitglieder unseres Führungsteams – einschließlich unseres CEO, Mike Salvino – einbezogen, um die Situation zu analysieren und wichtige Entscheidungen zu treffen. In solchen Zeiten ist gute Governance extrem wichtig. Wenn nicht klar ist, wer die Verantwortung trägt und wer für was zuständig ist, verrinnen wertvolle Minuten, die von den Angreifern für ihre Zwecke ausgenutzt werden.

Sprechen Sie frühzeitig mit den Behörden und mit Experten. Experten für Strafverfolgung und Sicherheit können Informationen von unschätzbarem Wert zum Abwehren von Angriffen und zu schnellen juristischen Gegenmaßnahmen bereitstellen. Beispielsweise war die Ransomware so aufgesetzt, dass von Xchanging Daten an Website-Domänen in den USA gesendet werden sollten. Also habe ich Kontakt zu Mitarbeitern der Strafverfolgungsbehörde aufgenommen, die an jenem Feiertagswochenende Dienst hatten. An jenem Abend haben wir eine gerichtliche Verfügung erwirkt, die es uns erlaubte, die Kontrolle über die Internetdomänen der Angreifer zu übernehmen.

Setzen Sie alle Hebel in Bewegung – und zahlen Sie nicht. Die Behörden raten dringend von der Lösegeldzahlung ab. In den USA und im Vereinigten Königreich gibt es sogar Bestrebungen, Strafen für die Zahlung von Lösegeld einzuführen. In unserem Fall hatten die Angreifer nicht sofort Geld gefordert. Sie wollten verhandeln. Wir wussten, dass wir den Angriff schnell unterbunden hatten, wir wussten, dass sie nicht unsere Daten hatten, und wir wussten, dass Sicherungen vorhanden waren. Wir waren in einer starken Position, daher mussten wir nicht verhandeln. Holen Sie sich unbedingt Hilfe, wenn Sie sich für Verhandlungen mit Cyber-Kriminellen entscheiden. Suchen Sie sich – im Idealfall im Rahmen der Vorbereitung auf Störungen, bevor der Angriff stattfindet – einen Verhandlungsführer, der Erfahrung mit Ransomware-Fällen hat, und arbeiten Sie mit diesem zusammen.

Gehen Sie offen mit dem Vorfall um. Sie müssen nicht alle Fakten offenlegen, aber Offenheit ist im Allgemeinen zu empfehlen. Wir haben die Indicators of Compromise (IoCs) der Angreifer Hunderten von Kunden bereitgestellt. Zweifellos gibt es Informationen, die Sie nicht weitergeben dürfen (wenn diese z. B. einer Vertraulichkeitsvereinbarung mit einem Kunden unterliegen oder wenn Sie von den Strafverfolgungsbehörden entsprechende Anweisungen erhalten haben). Wenn Sie Informationen, für die das möglich ist, anderen bereitstellen, hat dies jedoch mehrere Vorteile: Andere können sich schützen und Sie erhalten möglicherweise Hilfe von zahlreichen Kollegen, Behörden und der Sicherheits-Community. Am Sonntag, den 5. Juli, haben wir eine Pressemitteilung veröffentlicht, um die öffentlichen Märkte zu informieren. Einige Wochen später haben wir in einer weiteren Pressemitteilung die Eindämmung bestätigt.

Die Mitarbeiter der Strafverfolgungsbehörde, mit denen ich an jedem Wochenende gesprochen habe, waren überrascht, dass der Angriff auf unser Unternehmen bereits eingedämmt war. Die meisten Anrufe, die sie erhalten, werden vom CEO getätigt, da die IT- und Sicherheitsteams extrem beschäftigt sind. Normalerweise steht der Betrieb in den Unternehmen schon drei oder vier Tage lang still und es ist kein Ende abzusehen.

Wir wissen, dass der Angriff auf unser Unternehmen am 4. Juli viel schlimmer hätte laufen können. Die Kombination aus schneller Reaktion auf die Störung, Sicherheitskontrollen und Governance sowie der Nutzung von technischen Tools und branchenüblichen Verfahren hat uns einen Vorteil verschafft.

Die „neue DXC“ hat Stärke bewiesen. So konnten wir die Herausforderung bewältigen, ohne unsere oberste Priorität aus den Augen zu verlieren – unsere Kunden.

Und das war mein Sommerurlaub.

Informieren Sie sich über die neuesten Bedrohungen. Abonnieren Sie den DXC Bericht zu Sicherheitsbedrohungen unter **www.dxc.technology/threats_HBR**.

Über den Autor

Mark Hughes ist Senior Vice President, Offerings and Strategic Partners bei DXC Technology. Er ist weltweit für die Organisation und Angebote im Bereich Sicherheit verantwortlich. Dazu gehören die Abwehr von Cyber-Angriffen, geschützte Infrastrukturen, die digitale Identität und der Datenschutz. Zuvor war er in leitender Position bei BT Security tätig.

DG_8078a-21. Dezember 2020