DELL Technologies

Lehren aus einem Ransomware-Angriff

an der Autonomen Universität Barcelona

Gonçal Badenes
CIO, Autonome Universität Barcelona.
Das Interview wurde aus Gründen der Übersichtlichkeit gekürzt und bearbeitet.

Schnelles Handeln, Transparenz und ein gestärktes Bewusstsein für die Wichtigkeit einer Aktualisierung der Cybersicherheit prägten die Reaktion der Universität auf einen Ransomware-Angriff.

Sameer Shah, Dell Technologies Cybersecurity Marketing, hat mit CIO Gonçal Badenes über den Vorfall gesprochen.

Shah: Wir haben in letzter Zeit öfter darüber gesprochen, wie wichtig es ist, Organisationen dabei zu unterstützen, den Reifegrad ihrer Cybersicherheit schrittweise zu erhöhen. Sie wurden vor einiger Zeit Opfer eines Cyberangriffs. Bevor wir näher auf den Angriff eingehen, können Sie uns etwas über die Universität und ihre IT-Umgebung erzählen?

Badenes: Die Autonome Universität Barcelona ist eine der führenden Universitäten Spaniens. Die IT-Abteilung beaufsichtigt alle Services, die für den Betrieb der Universität erforderlich sind.

Direkt vor dem Angriff hatten wir einen vollständigen Plan zur Verbesserung unserer Cybersicherheitsmaßnahmen erstellt. Wir hatten die Multi-Faktor-Authentifizierung (MFA) implementiert, jedoch nicht für alle Services und NutzerInnen. Die Studierenden und alle IT-MitarbeiterInnen verfügten bereits über MFA, allerdings nur auf der Microsoft 365-Plattform. Andere Services waren nicht geschützt. Das Fehlen universeller MFA war ein wichtiger Faktor, wie wir später noch sehen werden.

Wann fand der Angriff statt und um welche Art von Angriff handelte es sich?

Es handelte sich um einen Ransomware-Angriff, der an einem langen Wochenende stattfand, wie es für diese Angriffe üblich ist. Gegen vier Uhr morgens erhielt ich einen Anruf von meinem Team. Man sagte mir, dass alle Services wie Dominosteine nacheinander ausfallen würden. Das Team schlug Alarm und wir versammelten sofort das Reaktionsteam, das wir für diese Fälle zusammengestellt hatten.

Woher wussten Sie, dass es sich um einen Ransomware-Angriff handelte? Gab es eine Lösegeldforderung?

Es gab Lösegeldforderungen auf den betroffenen Systemen. Und es gab einen kleinen Angriff, bei dem ein Skript zur Verschlüsselung von Computern ausgeführt wurde, die über das Wochenende online waren. Die Auswirkungen hiervon waren begrenzt und der Hauptzweck bestand wahrscheinlich darin, sicherzustellen, dass auch die MitarbeiterInnen und Studierenden von dem Angriff erfahren, nicht nur das IT-Team.

Hat Ihre Organisation zu irgendeinem Zeitpunkt die Zahlung des Lösegelds in Betracht gezogen?

Nein.

Warum nicht?

Das war aus ethischer Sicht nicht vertretbar. Glücklicherweise hatten wir Backups: zwei Kopien in zwei verschiedenen Rechenzentren auf dem Campus und eine dritte Kopie auf Band außerhalb des Perimeters der Organisation.

Bei diesen Backups handelte es sich um keinen Daten-Vault, richtig?

Nein, zu diesem Zeitpunkt hatten wir noch keinen Vault. Das war als zukünftige Priorität auf der Roadmap vermerkt. Aber dann wurde dieser Punkt [nach dem Angriff] natürlich priorisiert.

Eine gute Kommunikation kann in solchen Situationen entscheidend sein. Es klingt so, als wären Sie dem Angriff zuvorgekommen, indem Sie klar und transparent kommuniziert haben, auch mit den Medien?

Ja, vom ersten Tag an. Wir mussten vollkommen transparent und so offen wie möglich sein und erklären, was passiert war. Wir haben dafür gesorgt, dass andere sich vorbereiten und aus unseren Erfahrungen lernen können. Meine Vermutung ist, dass jemand von der Presse die Lösegeldforderung tatsächlich gelesen und die AngreiferInnen kontaktiert hat. Wir haben das nämlich nicht getan. Die AngreiferInnen gaben sich als die Gruppe PYSA (Protect Your System Amigo) zu erkennen.

Oft bevorzugen Organisationen es, solche Vorfälle geheimzuhalten, um eine Offenlegung ihrer Schwachstellen oder Korrekturtaktiken zu vermeiden. Hatten auch Sie da Bedenken?

Das sind sehr berechtigte Bedenken. Aber ich bin mir ziemlich sicher, dass uns allen bewusst ist, wie verwundbar wir sind. Wenn wir versuchen, unser Haus zu sichern, wissen wir, dass entschlossene Eindringlinge selbst die beste Tür auf dem Markt irgendwie aufbrechen können oder einen anderen Weg finden werden, um einzudringen. Das hier ist genau dasselbe.

Es ist keine Schande, dass wir angegriffen wurden und Schwachstellen hatten. Es ist wichtig, die Tatsache zu teilen, dass wir eine sehr klare Sicherheitsroadmap hatten und trotzdem Opfer eines Angriffs wurden. Selbst mit exzellenten Schutzmaßnahmen hätte es immer noch Sicherheitslücken gegeben, die man ausnutzen hätte können. Durch die Implementierung zusätzlicher Schritte kann man seine Position bedeutend stärken.

Erzählen Sie uns, welche Sofortmaßnahmen Sie ergriffen haben, um das Problem anzugehen.

Wir haben das Netzwerk heruntergefahren, alle Systeme. Wir haben uns an die Polizei und die regionale Datenschutzbehörde gewandt, dazu sind wir rechtlich verpflichtet. Und dann haben wir sofort zwei Teams in Aktion gerufen: Forensik und Wiederherstellung. Wir haben bei Dell angerufen und das Problem wurde sofort mit höchster Priorität eskaliert. Wir bekamen ein wirklich großartiges Team an die Seite gestellt, das ununterbrochen an der Sache gearbeitet hat. Diesem Team ist es gelungen, alle Daten auf der zweiten Data Domain vollständig wiederherzustellen.

Die Forensik begann also während des Wiederherstellungsvorgangs?

Einige Wiederherstellungsprozesse erforderten etwas Wartezeit. Deshalb sage ich, dass die Forensik zuerst gestartet wurde. Alles wurde unter Quarantäne gestellt, weil man schließlich herausfinden muss, was genau passiert ist. Wir mussten ein weiteres System zusammenstellen, damit wir Bestandteile nacheinander wieder online bringen konnten. Wir waren zu dem Schluss gekommen, dass alle Systeme, die online gehen, auch den höchsten Sicherheitsstandards entsprechen müssen, auch wenn das dann etwas länger dauert.

„Ich glaube, uns muss vor allem bewusst sein, dass es eine erhebliche Wahrscheinlichkeit dafür gibt, dass wir alle früher oder später Opfer eines Cyberangriffs werden. Daher müssen wir einen detaillierten Plan zur Risikominderung und Wiederherstellung haben."

Sie haben erwähnt, dass MFA nur auf Microsoft 365 verfügbar war und das mit ein Grund war, dass der Angriff möglich wurde. Ist jetzt flächendeckend MFA vorhanden?

Der Angriffsvektor war ein Benutzer mit kompromittierten Zugangsdaten, der in einem Team war, das auf Microsoft bereits MFA hatte. Als die AngreiferInnen versuchten, auf die E-Mail-Adresse zuzugreifen, und merkten, dass das aufgrund von MFA nicht möglich war, setzten sie ihre Suche jedoch fort. Und sie fanden heraus, dass wir einen VPN haben, der nicht durch MFA geschützt war. Sobald sie Zugang über den VPN hatten, konnten sie mit dem Ausloten des Netzwerks beginnen.

In unserem sehr großen Netzwerk fanden sie ein System mit einer Schwachstelle, was die laterale Ausbreitung ermöglichte. Zu Beginn der Wiederherstellung von Systemen haben wir also beschlossen, nichts mehr online zu schalten, das nicht mittels MFA geschützt ist.

Wenn Sie Ihren FachkollegInnen EINEN wichtigen Ratschlag zur Vermeidung eines Ransomware-Angriffs mit auf den Weg geben könnten, welcher wäre das?

Es ist sehr schwierig, einen einzigen Ratschlag zu geben. Ich glaube, uns muss vor allem bewusst sein, dass es eine erhebliche Wahrscheinlichkeit dafür gibt, dass wir alle früher oder später Opfer eines Cyberangriffs werden. Daher müssen wir einen detaillierten Plan zur Risikominderung und Wiederherstellung haben.

Zum Beispiel ist es sehr wichtig, die Kontaktdaten der wichtigsten Partner in den Bereichen Forensik und Wiederherstellung zur Hand zu haben, über eine detaillierte und priorisierte Karte der Services mit einem Zeitplan für die Wiederherstellung zu verfügen und außerdem eine gut abgestimmte Strategie mit den wichtigsten Geschäftseinheiten zu haben, einschließlich Kommunikation – sowohl intern als auch extern. Und natürlich ist es sehr wichtig, die BenutzerInnen zur Wachsamkeit anzuhalten und sie in Bezug auf die von AngreiferInnen verwendeten Techniken zu schulen.

Haben Sie das Gefühl, dass die Stärkung der Cybersicherheitsmaßnahmen an der Universität die Zuversicht in Bezug auf das Weiterverfolgen Ihrer Mission und Tätigkeiten gestärkt hat?

Absolut. Vor dem Angriff bestand unter anderem die Wahrnehmung, dass alle neuen Maßnahmen zum Schutz des Systems mit vielen Fragen und Bedenken bezüglich der tatsächlichen Erforderlichkeit aufgenommen wurden. Fakt ist, dass Schutz absolut notwendig ist, denn sonst bringt man seine gesamte Organisation in Gefahr. Natürlich glauben einige Leute immer noch, dass diese Maßnahmen ihre Arbeit behindern. Die meisten sind jedoch der Meinung, dass die Systeme viel besser geschützt sind.

Vielen Dank. Ihre Offenheit und Transparenz sind für alle von Vorteil, die daran arbeiten, den Reifegrad ihrer Cybersicherheit zu verbessern.