G DATA advanced analytics

Case Study

Vorfallsbewältigung an der RUB: Leitung eines **Incident Response Einsatzes** im Corona-Lockdown

RUHR UNIVERSITÄT BOCHUM RUB

Branche:
Universität

Umfang:
Mehr als 42.000 Studierende und über 6.000 hauptamtlich Beschäftigte an 21 Fakultäten

Standort:
Bochum, Deutschland

Herausforderung

- Schnelle Analyse des Netzwerks und Wiederherstellung der betroffenen Systeme nach einem Ransomware-Angriff
- IT-Security Consulting zur Verbesserung der IT-Sicherheit

Lösung

- Zusammenarbeit mit dem Incident Response Team von G DATA Advanced Analytics
- IT-Security Consulting zur Erhöhung des Sicherheitsniveaus nach Beendigung des Vorfalls

Vorteile

- Kompetente Soforthilfe vor Ort durch erfahrenes Personal
- Umfassendes Fachwissen in den Bereichen Vorfallsbehandlung, forensische Analyse und IT-Sicherheit

Mitten im ersten Corona-Lockdown legte ein Cyberangriff die Verwaltung der Ruhr-Universität Bochum (RUB) lahm. Mit Unterstützung von G DATA Advanced Analytics war die Universität schnell wieder handlungsfähig.

Kleine Lücke, große Wirkung: Eine einzige Schwachstelle reicht Cyberkriminellen aus, um Netzwerke von Unternehmen oder Organisationen zu infiltrieren. Das belegt der Cyberangriff auf die RUB. Dank aufmerksamer Mitarbeitenden und tatkräftiger Unterstützung des Incident Response Teams von G DATA Advanced Analytics konnte die Hochschule das Vorgehen der Angreifer analysieren und den Wiederanlauf der Systeme initiieren.

Am frühen Morgen des 7. Mai 2020 nahm das Unheil seinen Lauf. Mitarbeitende der zentralen IT an der RUB bemerkten, dass verschiedene Dienste, insbesondere SharePoint und Exchange, nicht mehr richtig funktionierten. Beim Überprüfen stellten sie fest, dass die Server teilweise verschlüsselt waren. Um eine weitere Ausbreitung zu verhindern, führten die Mitarbeitenden erste Sofortmaßnahmen durch und riefen den IT-Notfall aus. Die Verwaltung der RUB war damit arbeitsunfähig. Betroffen waren mehr als 42.000 Studierende und über 6.000 hauptamtliche Beschäftigte an 21 Fakultäten. Der einberufene Krisenstab entschied sich schnell, externe Fachleute zu Rate zu ziehen, um den Cyberangriff zu analysieren und die Systeme zu bereinigen. Die Wahl fiel dabei auf G DATA Advanced Analytics.

„Bei G DATA Advanced Analytics arbeiten glücklicherweise top ausgebildete IT-Sicherheitsfachkräfte,“ sagt Marcus Klein, Stellvertretender Direktor IT.SERVICES an der RUB. *„Sehr viele davon haben am Horst-Görtz-Institut studiert und ihren Abschluss gemacht, sodass wir um deren Kompetenzen wissen.“*

„Bei G DATA Advanced Analytics arbeiten glücklicherweise top ausgebildete IT-Sicherheitsfachkräfte. Sehr viele davon haben am Horst-Görtz-Institut studiert und ihren Abschluss gemacht, sodass wir um deren Kompetenzen wissen.“

Marcus Klein, Stellvertretender Direktor IT.SERVICES an der RUB

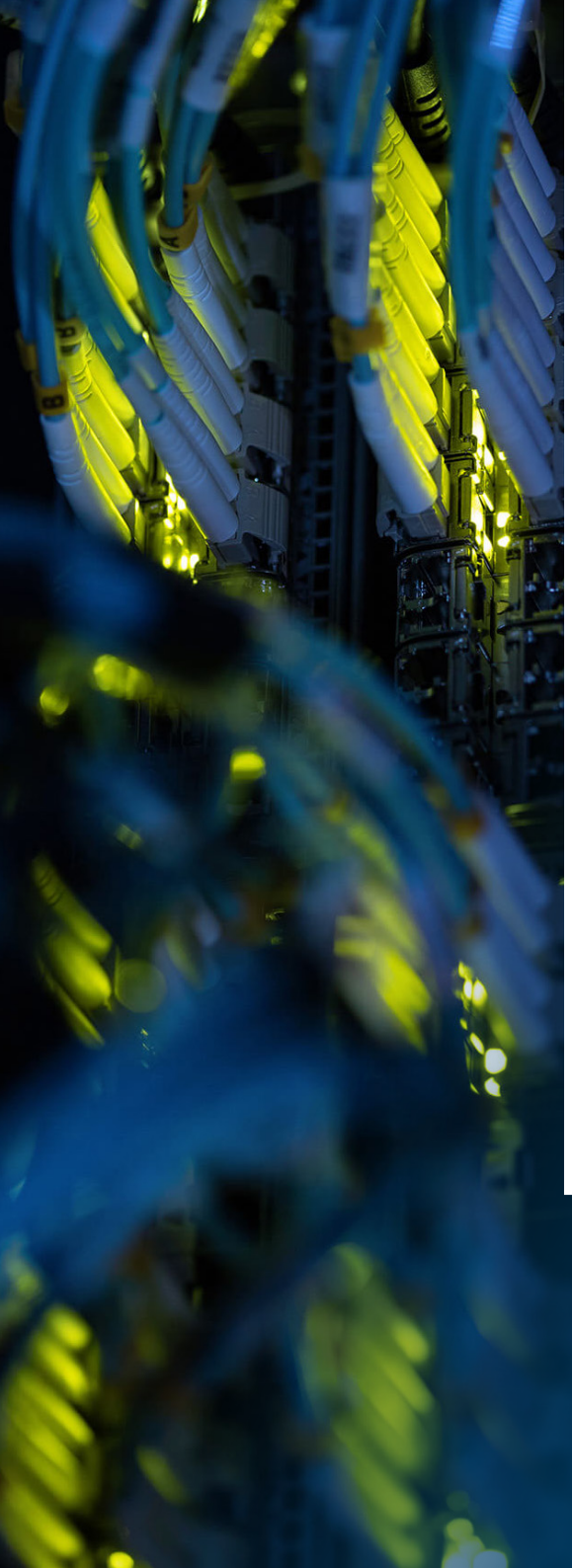
Dem Täter auf der Spur

Innerhalb kürzester Zeit nahm das Incident Response Team die Arbeit auf und analysierte die kompromittierten Systeme. Ausgehend von wichtigen Systemen, wie beispielsweise den Domänencontrollern, wurden die Spuren der Angreifer, soweit möglich und nötig, Schritt für Schritt nachverfolgt. So ergab der Blick in die Windows Event Logs, dass verschiedene PowerShell-Skripte ausgeführt wurden. Die Angreifer platzierten Schadsoftware auf mehreren Systemen, um darüber Funktionalität, wie beispielsweise die Erhöhung der Zugriffsrechte oder das Auslesen der Passwörter weiterer Benutzerkonten, zu nutzen. Da die verwendete Schadsoftware typischerweise nur im Arbeitsspeicher läuft, ist sie für Antivirenlösungen, die nur Festplatten untersuchen, nicht zu identifizieren. So konnten sich die Angreifer weiter ungestört im Netz ausbreiten. Durch die Analyse dieser sowie von weiterer gefundener Schadsoftware konnten die externen Serversysteme der Angreifer bestimmt werden. Über das gute Monitoring des Network Operation Centers der RUB wurden alle Systeme, die den Angreifern Zugangsmöglichkeit zum internen Netz boten, identifiziert und abschließend isoliert.

Der Tathergang

Die Analyse zeigte, dass der initiale Zugang in das Netz der RUB Anfang Mai über den Remotedesktopdienst eines Arbeitsplatzrechners erfolgte. Durch das simple Ausprobieren von Passwörtern, einem sogenannten Brute-Force-Angriff, erlangten die Angreifer die Zugangsdaten eines Benutzerkontos und damit Zugriff auf das System. Die Angreifer profitierten davon, dass das betroffene Konto administrative Rechte besaß und konnten sich so Informationen zu weiteren Benutzerkonten beschaffen. Eines dieser Benutzerkonten ermöglichte den Angreifern Zugriff auf den Domänencontroller der Unterdomäne. Von hier gelangten sie weiter auf die zentralen Server der RUB. Für einen dauerhaften Zugang zum internen Netz der RUB wurden durch die Angreifer mehrere eigene Benutzer angelegt, um sich weiter in der Infrastruktur umzusehen. Zusätzlich wurde Software auf mehreren Servern installiert, die einen weiteren Kommunikationskanal zu einem System der Angreifer herstellt. Anschließend begannen die Angreifer damit die Server automatisiert mit der Ransomware REvil zu verschlüsseln. Falls die Ransomware durch die Antivirenlösung gestoppt wurde, deaktivierten die Kriminellen den Virenschutz und starteten die Verschlüsselung ein zweites Mal. Der Vorfall wurde schließlich entdeckt, da zentrale Dienste, wie die Exchange-, SharePoint- und diverse Datenbankserver, nach der Ausführung der Ransomware nicht mehr funktionsfähig waren.

„Den Angreifern hat im Frühjahr 2020 die Corona-Pandemie in die Hände gespielt,“ sagt Jasper Bongertz, Head of Incident Response bei G DATA Advanced Analytics. *„Denn zu diesem Zeitpunkt hatten viele Unternehmen ihre Mitarbeitende schnellstmöglich ins Homeoffice beordert. Bei diesem Wechsel standen insbesondere die Stabilität und Funktionalität an oberster Stelle. Dass sich bei einem derartigen Kraftakt auch manchmal unbeabsichtigte Sicherheitslücken auftun ist leider deswegen problematisch, weil Cyberkriminelle diese laufend automatisiert suchen und ausnutzen.“*



Wiederaufbau nach Plan

Auf Basis der Analyse des Incident Response Teams von G DATA Advanced Analytics konnten die IT-Mitarbeitenden der RUB mit den Aufräumarbeiten beginnen. Ein großer Teil der Arbeiten musste dabei aufgrund des ersten Corona-Lockdowns remote erfolgen. Dafür wurden entsprechende Kommunikationsstrukturen aufgebaut und regelmäßig Videokonferenzen durchgeführt, um Ergebnisse auszutauschen und das weitere Vorgehen abzustimmen. Zusätzlich kommunizierten die Beteiligten via Messenger und kompensierten auf diesem Weg den fehlenden E-Mail-Kontakt.

Für den Wiederaufbau hatten die Beteiligten ein Konzept erstellt und eine Reihenfolge für den Wiederanlauf der Systeme festgelegt, welche die Mitarbeitenden der RUB nun nacheinander abarbeiteten. Das Wiederherstellen der verschlüsselten Server gelang zügig. Dabei profitierte die Universität von einer guten Backup-Strategie, bei der die Backups physisch getrennt vom Netzwerk aufbewahrt werden. So hatten die Angreifer keinen Zugriff darauf und die Daten konnten nach der Neuinstallation der Systeme direkt eingespielt werden.

Ein weiterer Vorteil: Ein eingespieltes Team im operativen Bereich mit dem notwendigen Know-how, um die Systeme aufzuräumen. So war beispielsweise der neue Domänencontroller bereits nach kurzer Zeit wieder einsatzbereit und wenig später waren auch die neuen Strukturen innerhalb der Domäne etabliert.

Mitte Juni waren alle essentiellen Systeme durch die Mitarbeitenden der RUB wieder hergestellt. Abschließend kann gesagt werden, dass die Entscheidung der Hochschulleitung nicht auf die Forderungen der Kriminellen einzugehen, die Richtige war.

IT-Sicherheit verbessern

Zusätzlich zu den Aufräumarbeiten plante der verantwortliche IT-Bereich gemeinsam mit G DATA Advanced Analytics zusätzliche Maßnahmen, um die IT-Sicherheit der RUB zu verbessern.

„Der Cyberangriff hat gezeigt, dass keine Organisation sich in Sicherheit wiegen kann,“ sagt Marcus Klein. *„Um uns zukünftig besser auf eine Attacke auf unsere IT-Systeme vorzubereiten, haben wir den aktuellen Status auf den Prüfstand gestellt und Maßnahmen definiert, die unseren IT-Schutz auf ein besseres Niveau heben und uns gleichzeitig in die Lage versetzen, angemessen zu reagieren, falls Cyberkriminelle in unsere Systeme eindringen.“*

Eine wesentliche Entscheidung war, die neue Windows-Domäne komplett zentral zu verwalten. Zusätzlich wurden die administrativen Berechtigungen der Fakultäten innerhalb Ihres Bereiches beschränkt, um etwa neue Mitarbeitende selbstständig anlegen und Gruppenzuordnungen bearbeiten zu können. Um Fernzugriffe zukünftig besser abzusichern, wurde eine neue Richtlinie für den Remotedesktopdienst erstellt und umgesetzt. Damit Vorfälle früher entdeckt werden, wurde als weiterer Punkt eine Sicherheitsüberwachung der wichtigen Systeme eingeführt. Des Weiteren wurde beschlossen, das interne Netzwerk neu zu segmentieren und weiter abzusichern. Eine Verbreitung innerhalb des Netzes (Lateral Movement) wird den Angreifern dadurch erschwert. Und nicht zuletzt entschied die IT-Abteilung, Awareness-Schulungen einzuführen, um das Bewusstsein der Angestellten für Cyberrisiken zu verbessern.