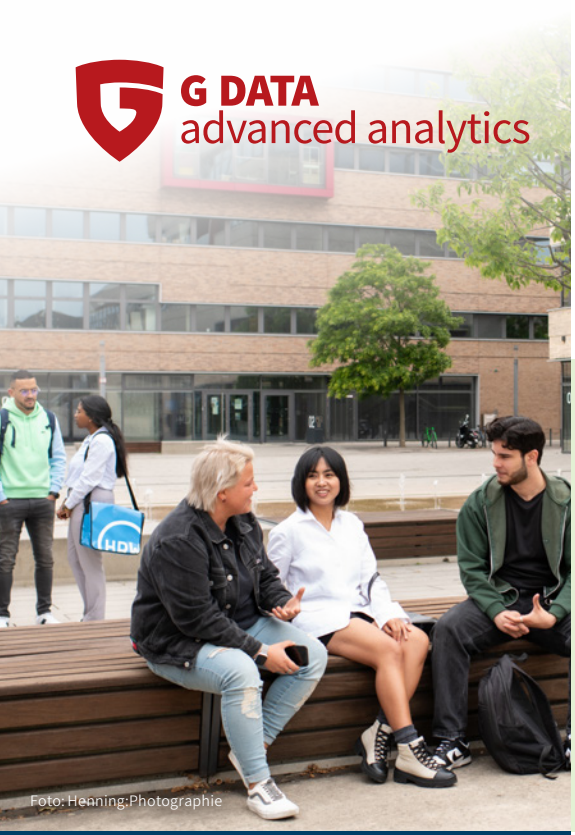
G DATA advanced analytics



Case Study

Cyberangriff auf die Hochschule Ruhr West

G DATA Advanced Analytics sorgt für reibungslosen Wiederaufbau des Netzwerkes

Herausforderung

- Forensische Spurensuche und Unterstützung beim Wiederanlauf der IT nach einer Cyberattacke

Lösung

- Incident Response von G DATA Advanced Analytics

Vorteile

- Strukturiertes Vorgehen bei der Bewältigung des IT-Sicherheitsvorfalles
- Einsatz von spezialisierten Werkzeugen zur Bereinigung der infizierten Systeme

HRW HOCHSCHULE RUHR WEST UNIVERSITY OF APPLIED SCIENCES

Branche:
Hochschule

Umfang:
600 Mitarbeitende
Über 6.500 Studierende

Standort:
Mülheim an der Ruhr
und Bottrop

Als ein Cyberangriff die Hochschule Ruhr West traf, handelten die IT-Mitarbeitenden schnell. Sie trennten die Systeme vom Netz, um Schlimmeres zu verhindern. Gleichzeitig beauftragte die IT-Leitung das Incident-Response-Team von G DATA Advanced Analytics. Das Bochumer Cyber-Defense-Unternehmen analysierte den Vorfall und half bei der Bereinigung der IT-Systeme von der Schadsoftware. So war die Hochschule schnell wieder handlungsfähig.

Hochschulen und Universitäten sind für Cyberkriminelle ein attraktives Ziel. Nachdem es bereits andere renommierte Institute wie die Ruhr-Universität Bochum, die Universität Duisburg-Essen und die Fachhochschule Münster getroffen hat, erwischte es im Februar 2023 auch die Hochschule Ruhr West. Glücklicherweise konnten die IT-Angestellten den Angriff schon frühzeitig stoppen und damit eine großflächige Ausbreitung sowie eine Verschlüsselung ihrer Systeme verhindern.

Schnelles Handeln verhindert Schlimmeres

Ein Mitarbeiter bemerkte bei Routinearbeiten ungewöhnliche Aktivitäten im System. Daraufhin entschieden die Verantwortlichen, das Netzwerk vom Internet zu trennen, um den Vorfall zu untersuchen. Bei einer genauen Prüfung bestätigte sich der Anfangsverdacht einer Cyberattacke mit Ransomware. An diesem Punkt informierte die Hochschule umgehend die Ermittlungsbehörden und beauftragte das Incident-Response-Team von G DATA Advanced Analytics mit der Vorfallbewältigung und der forensischen Analyse des Tathergangs. Darüber hinaus sollten die Fachleute die Schadsoftware untersuchen, um eine Re-Infektion beim Wiederaufbau zu verhindern.

Bei der Wahl des Partners folgten die Verantwortlichen dem Rat der Ermittlungsbehörden, einen vom BSI zertifizierten Dienstleister zu beauftragen. „Durch die Angriffe auf andere Hochschulen waren wir bereits vorgewarnt“, sagt Thomas Bieker, CIO der Hochschule Ruhr West. „Es war nur eine Frage der Zeit, bis es auch uns erwischt.Die Nachricht war trotzdem ein Schock für uns.“

„Die Fachleute haben uns einen roten Faden an die Hand gegeben, um die Kontrolle wieder zu erlangen. Gleichzeitig hat uns die Analyse geholfen, das Vorgehen der Tätergruppe zu verstehen.“

Thomas Bieker
CIO | Hochschule Ruhr West

Die Schwerpunkte der Hochschule Ruhr West mit ihren Standorten in Mülheim an der Ruhr und Bottrop liegen in den Bereichen Informatik, Ingenieurwissenschaften, Mathematik, Naturwissenschaften und Betriebswirtschaftslehre.
Über 6.500 Studierende werden in 33 Studiengängen ausgebildet – anwendungsbezogen, nachhaltig und vernetzt. So profitieren Studierende von der Forschungsstärke und Praxisnähe im Studium.

Priorisierter Wiederaufbau

Mit der Trennung vom Netz war die Hochschule nicht mehr arbeitsfähig. Da aber keine Daten verschlüsselt worden waren, konnten die Fachleute schnell mit dem Neuaufbau beginnen. Die Kriminellen hatten die Verschlüsselung noch nicht gestartet, da sie trotz intensiver Suche keinen Zugriff auf die Backup-Server erlangen konnten. Zu Beginn mussten alle Angestellten neue Passwörter setzen. Gemeinsam erarbeitete der Krisenstab einen Aktionsplan, um die Systeme nach und nach neu aufzusetzen. Da der Angriff die Hochschule zum Beginn der Prüfungsphase traf, galt für diese Systeme die höchste Priorität. Parallel entschieden die Verantwortlichen, die Prüfungen um eine Woche zu verschieben, um mehr Zeit für die anstehenden Arbeiten zu haben. Die Kommunikation mit den Studierenden und der Belegschaft erfolgte in der Anfangsphase über eine extern gehostete Webseite , mit Videobotschaften der Präsidentin sowie über ein paralleles E-Mail-System. All diese Maßnahmen sorgten für einen ruhigen Umgang mit der Krise.

„Das strukturierte Vorgehen von G DATA war sehr hilfreich“, sagt Thomas Bieker. „Die Fachleute haben uns einen roten Faden an die Hand gegeben, um die Kontrolle wieder zu erlangen. Gleichzeitig hat uns die Analyse geholfen, das Vorgehen der Tätergruppe zu verstehen.“

Den Tätern auf der Spur

Parallel dazu untersuchten die Incident-Response-Fachleute von G DATA Advanced Analytics eingehend die infizierten Systeme. Sie suchten gezielt nach Spuren, die einen Rückschluss darauf zuließen, wie die Angreifergruppe in die Systeme eindringen konnte. Dabei kamen auch spezielle, aus eigener Entwicklung stammende Werkzeuge zur Auswertung der Logdaten zum Einsatz. Das Team suchte gezielt nach Indicators of Compromise (IoCs), also Hinweisen, Daten und Konten, die Aufschluss über die Kompromittierung des Netzwerks geben konnten. Da die Logdaten nicht sehr weit in die Vergangenheit zurückreichten, ließ sich nicht der gesamte Angriffsweg rekonstruieren. Allerdings war erkennbar, dass der finale Angriff auf die Systeme durch ein kompromittiertes VPN-Konto eines Studierenden initiiert wurde. Die Analyse zeigte auch, dass die Tätergruppe mittels einer installierten Hintertür (Backdoor) versucht hat sich einen dauerhaften Systemzugriff zu sichern.

Foto: Henning:Photographie

Tipps für mehr IT-Sicherheit

In der Anfangsphase halfen die Fachleute aus Bochum dabei, einen stabilen Notbetrieb zu etablieren. Hierbei setzte das Team ein Werkzeug für Live-Forensik ein, um mittels individueller Suchkriterien netzwerkweite angeschlossene Systeme auf eine Kompromittierung zu überprüfen. So stellten die Expertinnen und Experten sicher, dass die Angreifer vollständig aus dem Netz verschwunden sind und keine unerkannte Schadsoftware den Wiederaufbau behindert. Für den Wiederaufbau der Systeme gaben sie konkrete Hinweise zur unmittelbaren Verbesserung des IT-Sicherheitsniveaus. Dazu zählte der Einsatz von Multi-Faktor-Authentifizierung für Mitarbeitende und Studierende, der Aufbau eines zentralen Log-Management-Systems, die strikte Trennung von administrativen und nicht-administrativen Konten sowie eine stärkere Netzwerk-Segmentierung.

Angriffe dauerhaft abwehren

Auf Basis dieser Empfehlungen arbeitet die IT-Abteilung daran, das Netzwerk für künftige Angriffsversuche besser abzusichern. Ziel ist es dabei, Sicherheitsstandards zu etablieren, die den Vorgaben des BSI entsprechen. So erhalten beispielsweise Dozierende nur noch temporär administrative Rechte für ihren Bereich, um etwa neue Software oder Updates zu installieren. Auch der externe Zugang zu Messgeräten in Laboren ist stärker reguliert. „Diese neue Vorgaben erhöhen den administrativen Aufwand deutlich“, sagt Thomas Bieker. „Aber gleichzeitig führt kein Weg daran vorbei, wenn wir unsere komplexe und heterogene Infrastruktur vor künftigen Angriffsversuchen schützen wollen. Denn wir sind jeden Tag Ziel von Cyberattacken und konnten bis jetzt jeden weiteren Angriffsversuch abwehren.“

Foto: Henning:Photographie