Stadt Hamm – Verteidigungsfähig dank G DATA CyberDefense

Mit Forensikern und Analyse-Tools hilft G DATA CyberDefense der Stadt Hamm, sich gegen Cyberattacken abzusichern.

Kunde

- Stadt Hamm
- Umfang: 2.500 Clients, 2 Rechenzentren

Die Herausforderung

- Schnelle und fachkundige Unterstützung im Schadensfall
- Ein individuelles Analyse-Tool, dass die Anforderungen der Stadt Hamm berücksichtigt

Die Lösung

- IT-Forensiker in Rufbereitschaft
- PXE-fähige Boot-CD zur Prüfung infizierter und gereinigter Geräte
- Maßgeschneiderte Softwarelösungen zur Integration in bestehende Infrastruktur und Prozesse

Die Vorteile

- Schnelle Hilfe im Schadensfall
- Kostenersparnis durch proaktives Handeln
- Tiefgehendes Vorwissen über IT-Infrastruktur dank regelmäßiger Workshops

elephantastisch! Hamm:

Die Stadt Hamm hat ein umfangreiches IT-Sicherheitskonzept. Da die Mitarbeiter in der IT großflächige Ausfälle nach einem Cyberangriff nicht selbst beheben können, setzt die Kommune auf die Zusammenarbeit mit G DATA CyberDefense.

Die kreisfreie Stadt Hamm mit mehr als 180.000 Einwohnern liegt im Norden des Regierungsbezirks Arnsberg am Rande des Ruhrgebiets und der Metropolregion Rhein-Ruhr. Die IT unterstützt die 2.500 städtischen Mitarbeiter dabei, die vielfältigen Aufgaben der Kommune zu erfüllen. In der Kommunalverwaltung umfasst der Fachbereich, der den IT-Betrieb in zwei Rechenzentren sowie die Anwendungslandschaft IT verantwortet, 25 Mitarbeiter. Diese ist mit 350 Applikationen sehr breit gefächert und deckt dabei die Anforderungen der unterschiedlichsten Fachbereiche ab – vom Straßenverkehrsamt über die Stadtbücherei bis hin zum Bürgerservice und Stadtreinigung. Eine besondere Herausforderung an die IT ergibt sich aus dem Datenschutz sowie weiteren gesetzlichen Vorgaben wie etwa dem eGov-Gesetz. Eine Folge davon: Die Anwendungen und die darin verarbeitenden Daten sind in Silos voneinander getrennt.

Kein Fremdwort: IT-Sicherheit

Mit der Verabschiedung des eGov-Gesetzes hat die Stadt Hamm die Digitalisierung des Behördenwesens auf den Weg gebracht. Dabei liegt der Fokus bis 2022 zunächst auf Prozessen und Schnittstellen, um den Wunsch der Bürger nach einer digitalen Verwaltung mit Online-Services nach zu kommen. Innerhalb des Transformationsprozesses nimmt das Thema IT-Sicherheit einen hohen Stellenwert ein. Konkreter Auslöser waren die Cyberattacken auf Krankenhäuser, die im Februar 2016 die IT zahlreicher Kliniken zum Teil für mehrere Tage lahmgelegt hatten.

„Die erfolgreichen Cyberangriffe haben uns verdeutlicht, dass es nicht mehr ausreicht, sich alleine auf Abwehrmaßnahmen zu konzentrieren“, sagt Klaus-Dieter Poppe, Abteilungsleiter IT-Betrieb bei der Stadt Hamm. „Daher haben wir unser IT-Sicherheitskonzept um eine Frage erweitert: Was passiert, wenn es jemand geschafft hat, uns anzugreifen?“ Unter dieser Prämisse hat die IT-Abteilung der Stadt Hamm eine „Arbeitsgruppe Notfall“ ins Leben gerufen, um durchgängige Strukturen für IT-Störfälle aufzubauen. Ein wichtiger Baustein dabei: Eine Schutzbedarfsanalyse, um

die Maßnahmen nach Dringlichkeit zu priorisieren.

Wer hilft, wenn's brennt?

Im Rahmen der Schutzbedarfsanalyse hat die Stadt Hamm Prozesse und Vorgehensweisen für unterschiedlichste IT-Notfälle etabliert. Dabei legen die Verantwortlichen Wert auf sehr kurze Entscheidungswege, um handlungsfähig zu bleiben. Jeder IT-Mitarbeiter der AG Notfall ist berechtigt, den Notfallplan in Kraft zu setzen, sobald die notwendigen Kriterien erfüllt sind. Ein Teil des Notfallplans ist dabei die Zusammenarbeit mit IT-Fachbereichen aus den benachbarten Kommunen, um mit mehr personellen Ressourcen schneller Herr der Lage zu werden. Allerdings zeigte sich, dass die Unterstützung der benachbarten Kommunen auch seine Grenzen hat: Insbesondere die Wiederherstellung im „Worst Case", wie etwa ein weitreichender Systemausfall infolge eines Malware-Angriffs, lässt sich kaum bewerkstelligen.

Ein Grund dafür: Fehlendes Know-how. Auf Empfehlung der IT-Experten von der Fachhochschule Hamm und der Ruhr-Universität Bochum nahm die Stadt Hamm Kontakt mit G DATA CyberDefense auf. Denn die Experten haben sich insbesondere bei der Abwehr und Bewältigung von Cyberangriffen einen Namen gemacht. „Die Zusammenarbeit mit der Stadt Hamm demonstriert exemplarisch unseren umfassenden Cyber-Security-Ansatz," sagt Tilman Frosch von G DATA CyberDefense. „Um Unternehmen oder Behörden verteidigungsfähig aufzustellen, ist es neben der technischen Ertüchtigung der eingesetzten Systeme unbedingt notwendig, Mitarbeiter in das Sicherheitskonzept mitaufzunehmen."

> „Wir haben unser IT-Sicherheitskonzept um eine Frage erweitert: Was passiert, wenn es jemand geschafft hat, uns anzugreifen?"
>
> Klaus-Dieter Poppe, Abteilungsleiter IT-Betrieb

Infizierte Rechner checken

In einem initialen Workshop besprachen die Verantwortlichen daher die aktuelle Notfallstrategie sowie die Anforderungen an eine externe Unterstützung. Hier zeigten sich zwei Ansatzpunkte für eine Zusammenarbeit. Zunächst benötigte die Stadt Hamm im Falle einer erfolgreichen Ransomware-Attacke professionellen Support beim Incident Response. Vereinbart wurde eine Rufbereitschaft: Innerhalb eines festgelegten Zeitfensters sind Mitarbeiter von G DATA vor Ort und unterstützen die Angestellten in Hamm mit ihrem Fachwissen. Sie prüfen, wie die Malware ins Netzwerk eingedrungen ist und schließen bestehende Sicherheitslücken. Gleichzeitig helfen sie, den Schädling zu identifizieren, um weitere Details über das Angreifer-Vorgehen zu ermitteln und den Schaden zu begrenzen.

Unterstützung gibt es auch bei der Wiederherstellung der Systeme. Infizierte Systeme werden unmittelbar in ein separates Virtual Local Area Network (VLAN) verschoben, um eine weitere Ausbreitung zu unterbinden. Diese Systeme säubern die Spezialisten und nutzen dafür maßgeschneiderte G DATA Werkzeuge. Anschließend erfolgt ein Test mit der G DATA PXE (Preboot Execution Environment) Boot-CD, ob die Säuberung

erfolgreich war. Dieses Standardprodukt hat G DATA an die Bedürfnisse der Stadt Hamm angepasst und durch maßgeschneiderte Software in vorhandene Prozesse integriert. Das nun bereinigte System wird von dem VLAN zurück in das ursprüngliche Produktiv-Netz migriert. Die Verantwortlichen erhalten die Ergebnisse übersichtlich in Tabellenform und sehen auf einen Blick, welche Rechner wieder arbeitsfähig sind und zurück in das Produktivnetz überführt werden können.

„Dank der G DATA CyberDefense fühlen wir uns sehr gut auf eine Attacke vorbereitet", sagt Klaus-Dieter Poppe. „Wir stehen in einem engen Austausch, um unsere Notfallpläne aktuell zu halten. Denn IT-Sicherheit ist kein abgeschlossener Prozess, sondern bedarf kontinuierlicher Anpassungen. Schließlich schläft der Feind nicht."

Mehr Informationen:

www.gdata.de

TRUST IN GERMAN SICHERHEIT

G_DATA_CaseStudy_Stadt_Hamm_DE • 57141.10220