PROFI.referenz

ABWASSER- UND STRAßENREINIGUNS-BETRIEB DER STADT GIFHORN (ASG)

ASG

MEHR IT-SECURITY LÄSST HACKERN WENIG CHANCE

PROFI
Wir entwickeln mehr als IT

MAßNAHMEN-MIX SORGT FÜR BESTMÖGLICHEN SCHUTZ

Der ASG – Dienstleister für Abwasserbeseitigung und Straßenreinigung

Seit seiner Gründung im Jahr 1995 sorgt der Abwasser- und Straßenreinigungsbetrieb Stadt Gifhorn (ASG) als kommunaler Eigenbetrieb für eine sichere, umweltgerechte Abwasserbeseitigung und Straßenreinigung in Gifhorn. Zur Reinigung von Straßen, Gehwegen und Fahrradwegen zählt auch der Winterdienst. Darüber hinaus kümmert sich der ASG um die Veranlagung der Benutzungsgebühren für die Inanspruchnahme der Abwasserbeseitigung und Straßenreinigung. Die derzeit 48 Mitarbeitenden sind in den Bereichen Verwaltung und Straßenreinigung, Kanalbau und Grundstücksentwässerung sowie Abwasserreinigung organisiert.

Ausgangssituation und Ziele

Der ASG war mit der Unterstützung von PROFI bereits dabei, seine IT-Landschaft zu modernisieren und hatte diese mittels Highend-Firewall abgesichert, als das Unternehmen Ziel eines Cyberangriffs wurde. Im Einsatz waren virtuelle Server der neuesten Generation von VMware (ESXi) sowie eine ML (Machine Learning)-gestützte Firewall des Anbieters Palo Alto Networks. Allerdings waren lediglich zwei Brandabschnitte eingerichtet, bestehend aus einem produktiven sowie einem Backup-Server, aber keine Absicherung über die Cloud. Innerhalb kürzester Zeit legten die Angreifer zuerst das Backup- und danach das Hauptsystem lahm, sodass die Verwaltung des ASG nicht mehr arbeitsfähig war. Einfallstor der Attacke war die Software, die der Kunde für seine Remote-Arbeitsplätze einsetzte. Die für die Bürger relevanten und im Alltag bemerkbaren Dienstleistungen Abwasserbeseitigung und Straßenreinigung waren nicht betroffen, hier war der ASG uneingeschränkt handlungsfähig.

„Ein guter IT-Partner ist essenziell, um die Folgen einer Cyberattacke bewältigen zu können. Dank der Unterstützung von PROFI waren wir binnen kürzester Zeit wieder handlungsfähig und für die Bürger erreichbar.“

Peter Futterschneider,
Betriebsleiter ASG

"Zum Glück hatten wir schon vor dem Angriff begonnen, die IT-Landschaft des ASG zu modernisieren und so schlimmere Folgen verhindert. Wir sind sehr froh, dass wir die Attacke gemeinsam meistern konnten. Durch den umgesetzten Maßnahmen-Mix ist der ASG nun bestmöglich geschützt.“

Stefan Vieregge, Geschäftsfeldleiter
Hybrid IT Solutions der PROFI AG

Die PROFI-Leistung
Dank des hohen Digitalisierungsgrads des Kunden gelang es PROFI, die vom Cyberangriff betroffenen Systeme binnen fünf Tagen wiederherzustellen. Für den Restore nutzte PROFI die Cloud-Lösung von Amazon (Amazon Web Services, AWS) und migrierte schließlich die Systeme auf die On-Premise-Landschaft des Kunden. Der ASG war dann wieder für die Bürger erreichbar und konnte seine Verwaltungsarbeiten fortführen.

Um den ASG künftig besser gegen Cyberkriminelle zu schützen, installierte PROFI in enger Zusammenarbeit mit dem Kunden die folgenden Neuerungen:

Für ein großes Plus an IT-Sicherheit sorgt nun ein dritter Brandabschnitt in der Cloud-Lösung von Amazon am Standort Frankfurt. Ein Restore wäre im Katastrophenfall – wie bei einem erneuten Angriff – in nur vier Stunden möglich. Denn in diesem Zeitabstand repliziert die neu genutzte Disaster-Recovery-Funktion kritische, virtuelle Maschinen vollautomatisiert in die Cloud. Retention Lock bewirkt, dass kritische Daten nicht einfach bei einer Ransomware-Attacke überschrieben werden können. Selbst wenn man nach einem Angriff die Systeme bei einer reinen On-Premise-Lösung in nur vier Stunden wieder herstellen könnte (was sehr unwahrscheinlich ist), so wäre das nicht erlaubt. Denn physische Server werden vorerst von den Behörden als Beweismittel für einen Cyberangriff sichergestellt.

Zusätzliche Sicherheit gibt die neu eingerichtete Mikrosegmentierung der genutzten Firewall von Palo Alto Networks, wodurch nun separate Firewalls zwischen den einzelnen, virtuellen Servern bestehen.

Eine weitere Ebene der IT-Security, die organisatorische Sicherheit, verbesserte PROFI gemeinsam mit dem ASG durch zwei Maßnahmen: Zum einen führte man die Zwei-Faktor-Authentifizierung ein, zum anderen haben Administratoren nur noch Zugriff auf eine IT-Ebene, also etwa ausschließlich auf das Active Directory, die Server oder die Clients.

Fazit
Der ASG wurde Ziel eines Cyberangriffs, konnte dessen Folgen jedoch dank seines hohen Digitalisierungsgrads sowie der Unterstützung des IT-Dienstleisters PROFI in nur fünf Tagen in den Griff bekommen. Von der Attacke betroffen war die Verwaltung des kommunalen Dienstleisters, die nach einem Restore der Systeme in der neu genutzten Cloud-Lösung wieder voll handlungsfähig war. Um den ASG künftig besser vor Ransomware-Attacken zu schützen, setzte PROFI gemeinsam mit dem Kunden einen Mix an Maßnahmen um. Diese verbesserten die IT-Sicherheit auf verschiedenen Ebenen – technisch und organisatorisch. Zentrale Bestandteile des neuen Sicherheitskonzepts sind ein dritter Brandabschnitt in der Cloud sowie eine Disaster-Recovery-Funktion. Dieser Mix lässt Cyberkriminellen künftig wesentlich weniger Chancen auf Erfolg.

Kundennutzen

- Mehr IT-Sicherheit durch eine Kombination von Maßnahmen wie installierte Disaster Recovery, Mikrosegmentierung der Firewall und einen dritten Brandabschnitt in der Cloud.
- Zentral verwaltete, automatisierte Firewall-Funktionen sorgen für mehr Sicherheit und eine komfortable Steuerung.
- Verbesserte Einhaltung der IT-Compliance durch permanente Audits der neuen Infrastruktur.

Hintergrund: Die Ursache der Cyberattacke

Einfallstor der Cyberattacke auf die Systeme des ASG war vermutlich eine sogenannte Log4j-Lücke – eine kritische Schwachstelle in der viel genutzten Java-Bibliothek. Offensichtlich hatten Cyberkriminelle die Lücke erfolgreich ausgenutzt und zuerst das Backup- und danach das Produktivsystem des ASG übernommen. Das Vorgehen deutet darauf hin, dass sich der Angreifer schon länger im System befand. Angreifer wählen die Ziele für ihre Attacken meist zufällig aus, indem sie Sicherheitslücken in Systemen scannen. Zudem existieren gezielte Angriffe auf bestimmte Organisationen. Unternehmen verbessern ihren Schutz, indem sie alle Software-Updates (Patches) schnellstmöglich einspielen, denn auch Angreifer patchen regelmäßig die von ihnen genutzte Malware.

DIE PROFI ENGINEERING SYSTEMS AG

Wir, die PROFI Engineering Systems AG sind ein mittelständisches Familienunternehmen. Als finanzkräftiges IT-Lösungshaus mit Hauptsitz in der Wissenschaftsstadt Darmstadt sind wir seit über 35 Jahren der IT-Dienstleister für unsere Kunden, mit individuellen hochwertigen Lösungen zur Optimierung von IT-Prozessen und Systemlandschaften.

Wir begleiten Unternehmen bei der digitalen Transformation – von der IT-Strategie über die Implementierung bis einschließlich des Betriebes der Systeme und Plattformen. Unsere erfahrenen Berater und Architekten beschäftigen sich seit vielen Jahren intensiv mit der Digitalisierung aller Geschäftsabläufe und Unternehmensbereiche. Gestalten Sie mit den PROFI-Fokusthemen schon heute Ihre digitale Zukunft. Profitieren Sie von unserem Know-how vor allem im Kontext von Managed Services, Digital Workplace, SAP HANA, Business Continuity, Agile Software-Entwicklung, Netzwerk & Security, Cloud Solutions, SDDC & Agile Plattformen, Speicherlösungen und Server-Lösungen.

Wir übernehmen für Sie Projektmanagement und Implementierung, einschließlich dem Betrieb Ihrer Systeme und Plattformen. Unser Anspruch ist höchste Kompetenz, Zuverlässigkeit und Qualität, mit messbarem Erfolg und direktem Beitrag zur Wertschöpfung und Wettbewerbsfähigkeit unserer Kunden.

Seit vielen Jahren gehören wir zu Deutschlands erfolgreichsten IT-Lösungsanbietern und pflegen langjährige Partnerschaften mit führenden IT-Herstellern. Die PROFI Engineering Systems AG beschäftigt über 300 Mitarbeiterinnen und Mitarbeiter an 12 Standorten.

Unsere IT-Lösungen für Ihren Erfolg

- **Agile Software-Entwicklung**
- **Business Continuity**
- **Cloud Solutions**
- **Digital Workplace**
- **Managed Services**
- **SAP HANA**
- **SDDC & Agile Plattformen**
- **Security & Netzwerk**
- **Server-Lösungen**
- **Speicherlösungen**

PROFI Engineering Systems AG
Otto-Röhm-Straße 18
64293 Darmstadt
Telefon: +49 6151 8290-0
Telefax: +49 6151 8290-7610
E-Mail: profi@profi-ag.de
www.profi-ag.de

04/2023

UNSERE PARTNER

Gemeinsam mit unseren starken Partnern setzen wir Ihre optimalen Lösungen um.

IBM Platinum Partner
SAP Partner
Microsoft Partner – Gold Datacenter, Silver Cloud Productivity, Silver Communications, Silver Messaging, Silver Collaboration and Content
FUJITSU SELECT Expert
VEEAM PROPARTNER Gold Reseller
Data Center Partner Platinum Lenovo
DELL Technologies TITANIUM PARTNER
vmware Principal Partner Data Center Virtualization
cisco Premier Partner
Red Hat Premier Business Partner
NUTANIX RESELLER CHAMPION
NetApp Platinum Partner

Bildnachweise:
unsplash.com:
© Samara Doole: Titel

shutterstock.com:
© Sergey Nivens: S. 2

PROFI
Wir entwickeln mehr als IT