



Stärkung der Cybersicherheit mit automatischer Sofortreaktion gegen Ransomware



Eine große Hilfs- und Rettungsorganisation erhöht die Betriebsstabilität durch Minimierung der von zunehmenden Ransomware-Bedrohungen ausgehenden Risiken. Die Erkennung und Abwehr von Ransomware-Angriffen innerhalb von 15 Sekunden sorgt für einen zuverlässigen 24/7-Betrieb – ein wichtiger Schritt zum Retten von Leben und Senken von Cyberversicherungsprämien.

Über das Unternehmen und seine Herausforderung

Der DRK Landesverband Berliner Rotes Kreuz e. V. ist einer von 19 Landesverbänden im Deutschen Roten Kreuz. Als Teil der internationalen Rotkreuz- und Rothalbmondbewegung bietet das Berliner Rote Kreuz eine Vielzahl verschiedener sozialer Dienstleistungen an, darunter Ambulanz- und Transportdienste, Wasserrettung, Gesundheitsversorgung und Sozialhilfe.

Die 2.500 ehrenamtlichen und hauptamtlichen Mitarbeitenden des Berliner Roten Kreuzes und seiner acht Kreisverbände bearbeiten als Hilfskräfte der deutschen Behörden jedes Jahr Tausende von Notrufen. Die Hilfsgesellschaft unterhält außerdem acht Tochtergesellschaften, die älteren Menschen Unterstützung anbieten, und verteilt täglich etwa 600 Mahlzeiten, um eine gesunde Lebensweise zu fördern.

Als Rettungsdienst muss das Berliner Rote Kreuz zu jeder Zeit – sei es tagsüber oder nachts – schnell auf die jeweilige Situation reagieren. Kommunikation und Koordination sind entscheidend für den Schutz von Menschenleben und die Organisation muss ununterbrochen Zugang zu wichtigen Systemen und Dokumenten haben, um die Bürger in der Region und darüber hinaus zu schützen.



v.l.n.r.: Alexander Adamzik, Regional Director Small Medium Enterprise Division, Ricoh Deutschland GmbH, Chris Konczak, Stellv. Leitung zentrale Dienste – IT, DRK Landesverband Berliner Rotes Kreuz e.V., Peter Malchow, Kaufmännischer Leiter / Syndikus, DRK Landesverband Berliner Rotes Kreuz e.V., Marcel Richter, Leitung zentrale Dienste – IT, DRK Landesverband Berliner Rotes Kreuz e.V., Leonid Friedmann, Senior Account Manager Field Sales, Ricoh Deutschland GmbH.

Das Berliner Rote Kreuz ist beispielsweise auf Millionen digitaler Dateien angewiesen, darunter Zeitpläne, Dienstpläne, Rechnungen und vertrauliche Gesundheitsdaten, um wirksam helfen zu können. Dafür zu sorgen, dass diese Dokumente immer zugänglich und vor Cyberbedrohungen geschützt sind, ist eine der größten Herausforderungen für das IT-Team der Organisation.

Marcel Richter, Leiter Zentrale Dienste – IT beim Berliner Roten Kreuz, sagt: „Wir betreiben die IT für den Landesverband mit 26 Abteilungen und acht Tochtergesellschaften, und wir erbringen Dienstleistungen für drei Kreisverbände. Unsere Aufgabe ist es, die rund 650 ehrenamtlichen und hauptamtlichen Mitarbeitenden dabei zu unterstützen, den Berlinerinnen und Berlinern in denjenigen Momenten zu helfen, in denen sie Hilfe am meisten brauchen. In solchen Situationen zählt jede Sekunde, um Leben zu retten. Ausfallzeiten oder Ausfälle können schreckliche Folgen haben.“

Obwohl das Berliner Rote Kreuz noch keinen größeren Sicherheitsvorfall erlebt hatte, war es sich des wachsenden Risikos durch neue Cyberbedrohungen wie Ransomware mehr als bewusst. Um das Risiko zu minimieren und seine wichtigen Systeme zu schützen, wollte die Organisation eine zusätzliche Ebene des Cyberschutzes einführen.



Mehrere Organisationen, mit denen wir zusammenarbeiten, wurden von Ransomware befallen. Deshalb wollten wir alle möglichen Schritte unternehmen, um unsere Dienste zu schützen und sicherzustellen, dass wir die anspruchsvollen regulatorischen Auflagen erfüllen.

Chris Konczak

Stellvertretender Leiter Zentrale Dienste – IT
DRK Landesverband Berliner Rotes Kreuz e.V.



„Das Team von Ricoh ist immer hilfsbereit. Die Zusammenarbeit mit unserer Beschaffungsabteilung war ebenso hervorragend wie der technische Support und Ricoh hat uns bei der Präsentation des Lösungsvorschlags bei unseren Geschäftspartnern geholfen.“

Marcel Richter, Leitung zentrale Dienste – IT
DRK Landesverband Berliner Rotes Kreuz e.V.



Chris Konczak, stellvertretender Leiter Zentrale Dienste – IT beim Berliner Roten Kreuz, fügt hinzu: „Cyberangriffe machen Schlagzeilen, und die Wiederherstellung von Daten ist oftmals zeitraubend und teuer. In der Vergangenheit wurden Hilfsorganisationen von Cyberkriminellen verschont, aber jetzt werden wir aktiv ins Visier genommen, so dass wir uns entsprechend anpassen müssen, da Phishing- und andere Angriffe immer raffinierter werden. Mehrere Organisationen mit denen wir zusammenarbeiten, wurden von Ransomware befallen. Deshalb wollten wir alle möglichen Schritte unternehmen, um unsere Dienste zu schützen und sicherzustellen, dass wir die anspruchsvollen regulatorischen Auflagen erfüllen.“

Lösung

Das Berliner Rote Kreuz arbeitet seit vielen Jahren mit Ricoh zusammen und setzt multifunktionale Bürodrucksysteme ein. Da das Berliner Rote Kreuz mit der Servicequalität von Ricoh stets zufrieden war, beschloss es, die Zusammenarbeit auf Cybersicherheitslösungen auszuweiten und RICOH RansomCare powered by BullWall einzusetzen.

„Wir haben ein paar unterschiedliche Cybersicherheitsprodukte getestet und festgestellt, dass die meisten unseren Anforderungen nicht gerecht werden“, sagt Marcel Richter. „Wir wollten eine Lösung, die nicht vom

Einsatz spezieller Clients und Agents an verschiedenen Endpoints und Infrastrukturanlagen abhängig ist, da wir eine sehr heterogene Umgebung haben.“

Das Berliner Rote Kreuz führte einen Probelauf mit RansomCare durch und entschied sich schnell für die agentenlose Lösung zur Erkennung und Eindämmung von Bedrohungen. „Besonders gut hat uns die schnelle und einfache Inbetriebnahme von RansomCare gefallen“, sagt Chris Konczak. „Während andere Lösungen Funktionen zum Schutz vor Ransomware bieten, war RansomCare die einzige Speziallösung und entsprechend höher ist der Schutz, den RansomCare bietet.“

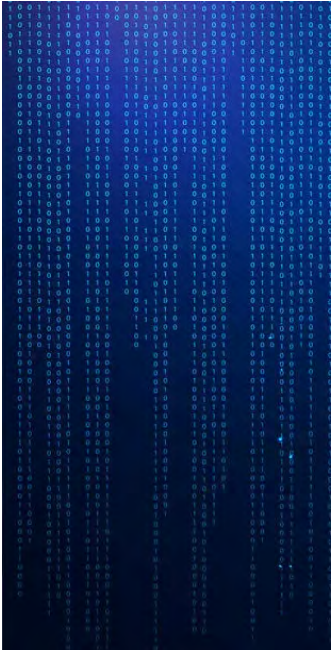
Heute lässt das Berliner Rote Kreuz RansomCare auf einer dedizierten virtuellen Maschine getrennt von anderen Workloads laufen, um optimale Leistung und Schutz zu gewährleisten. Die Lösung überwacht rund 650 Benutzer- und Funktionskonten, Millionen von Dateien und 80 virtuelle Maschinen, auf denen viele Anwendungen und Datenbanken laufen. Die von RansomCare geschützte Anwendungslandschaft besteht aus lokalen und Cloud-basierten Systemen, darunter Dateiserver, Microsoft SharePoint, Microsoft SQL Server und Microsoft 365.

Bei der Implementierung von RansomCare nutzte das Berliner Rote Kreuz die Standardeinstellungen, die eine solide Grundlage für die Abwehr von Ransomware-Angriffen bilden. „Die Lösung ist sehr anwenderfreundlich, und wir haben die



RansomCare hat sich schnell zu einem Eckpfeiler unserer Cybersicherheitsstrategie entwickelt und ergänzt perfekt unsere Endpoint-Sicherheit und unseren Virenschutz.

Marcel Richter, Leitung zentrale Dienste – IT
DRK Landesverband Berliner Rotes Kreuz e.V.



Konfiguration nur minimal angepasst“, erklärt Chris Konczak. „Wir haben RansomCare auch in unser Endpoint-Security-System von Sophos integriert. Wenn RansomCare verdächtige Aktivitäten erkennt, überträgt es die Eindämmungsmaßnahmen nahtlos an die Endpoint-Security-Lösung. Als nächsten Schritt planen wir, einen zweiten Knoten hinzuzufügen, auf dem RansomCare läuft, um eine hohe Verfügbarkeit zu gewährleisten und die Zuverlässigkeit und Cybersicherheit weiter zu optimieren.“

Vom ersten Gespräch an war das Berliner Rote Kreuz mit der Unterstützung von Ricoh mehr als zufrieden. „Das Team von Ricoh ist immer hilfsbereit“, bestätigt Marcel Richter. „Die Zusammenarbeit mit unserer Beschaffungsabteilung war ebenso hervorragend wie der technische Support und Ricoh hat uns bei der Präsentation des Lösungsvorschlags bei unseren Geschäftspartnern geholfen. Wir erhalten auch immer schnell Antworten auf unsere Fragen, meist innerhalb einer Stunde.“

Vorteile

Dank Ricoh und RansomCare hat das Berliner Rote Kreuz seinen Ransomware-Schutz erheblich verbessert, erklärt Marcel Richter: „RansomCare hat sich schnell zu einem Eckpfeiler unserer Cybersicherheitsstrategie entwickelt und ergänzt perfekt unsere Endpoint-Sicherheit und unseren Virenschutz. Mit RansomCare haben wir unsere Abwehr um eine weitere Ebene ausgebaut, um neue Cyberangriffe zu erkennen und darauf zu reagieren. Die hochgradig zielgerichteten und effektiven Isolierungs- und Eindämmungs-Tools helfen uns dabei, sicherzustellen, dass unsere Nutzer ununterbrochen Zugang zu unseren wichtigen Systemen und Dateien haben.“

Da das Berliner Rote Kreuz 24 Stunden am Tag, sieben Tage die Woche in Bereitschaft ist, wollte es eine vollautomatische Lösung, die keine ständige Überwachung durch sein IT-Team erfordert. RansomCare bietet genau das: Die Lösung überwacht rund um die Uhr mögliche

Bedrohungen und löst automatisch schnelle Eindämmungsmaßnahmen aus, die den Schaden effektiv minimieren. „Wir haben festgestellt, dass RansomCare jede potenziell gefährliche Aktivität innerhalb von 15 Sekunden blockiert“, erklärt Chris Konczak. „Keine andere Lösung, die wir gesehen haben, reagiert so schnell. Genau wie bei jeder anderen Notfallsituation sind eine schnelle Erkennung und Eindämmung das A und O. Und mit dem intuitiven Echtzeit-Dashboard in RansomCare können wir sofort sehen, was die Eindämmungsmaßnahme ausgelöst hat, und die Benutzer gegebenenfalls direkt kontaktieren.“

Ein weiterer großer Vorteil für das Berliner Rote Kreuz sind die integrierten Berichtsfunktionen von RansomCare. Im Falle eines Vorfalls kann die Organisation schnell und einfach zertifizierte Compliance-Berichte erstellen, um die Behörden zu informieren.

Marcel Richter zieht sein Fazit: „Mit Ricoh und RansomCare haben wir unsere IT-Sicherheit deutlich verbessert. Dies wird sich auch positiv auf unsere Cyberversicherungsprämien auswirken, bei denen wir dank RansomCare einen erheblichen Nachlass erwarten. Da wir lebensrettende Notfalldienste anbieten, stehen wir unter besonderer Beobachtung der Behörden, was die Gewährleistung der Betriebssicherheit betrifft. Mit dem Einsatz von RansomCare sind wir der Erfüllung der hohen Informationssicherheitsanforderungen des deutschen Bundesamtes für Sicherheit in der Informationstechnik einen Schritt nähergekommen.“

ÜBER RICOH

Ricoh unterstützt digitale Arbeitsplätze mit innovativen Technologien und Dienstleistungen, die es dem Einzelnen ermöglichen, von überall aus intelligenter zu arbeiten.

Mit fundiertem Wissen und organisatorischen Fähigkeiten, die in der 85-jährigen Geschichte des Unternehmens gewachsen sind, ist Ricoh ein führender Anbieter von digitalen Dienstleistungen, Informationsmanagement sowie Druck- und Bildgebungslösungen, die die digitale Transformation unterstützen und die Unternehmensleistung optimieren.

Die Ricoh-Gruppe hat ihren Hauptsitz in Tokio und verfügt über bedeutende Niederlassungen in der ganzen Welt. Ihre Produkte und Dienstleistungen erreichen Kunden in rund 200 Ländern und Regionen. In dem im März 2022 abgeschlossenen Geschäftsjahr erzielte die Ricoh-Gruppe einen weltweiten Umsatz von 1.758 Milliarden Yen (ca. 14,5 Milliarden USD).

Besuchen Sie unsere Website für weitere Informationen: www.ricoh.de

RICOH
imagine. change.

www.ricoh.de

Die Fakten und Zahlen in dieser Broschüre beziehen sich auf spezifische Geschäftsfälle. Individuelle Bedingungen führen eventuell zu abweichenden Ergebnissen. Alle Firmen-, Marken-, Produkt- und Servicenamen sind das Eigentum von und eingetragene Marken ihrer jeweiligen Eigentümer. Copyright © 2023 Ricoh Europe PLC. Alle Rechte vorbehalten. Diese Broschüre, deren Inhalt und/oder Layout dürfen ohne vorherige schriftliche Erlaubnis von Ricoh Europe PLC nicht verändert und/oder angepasst, teilweise oder vollständig kopiert und/oder in andere Dokumente eingefügt werden.