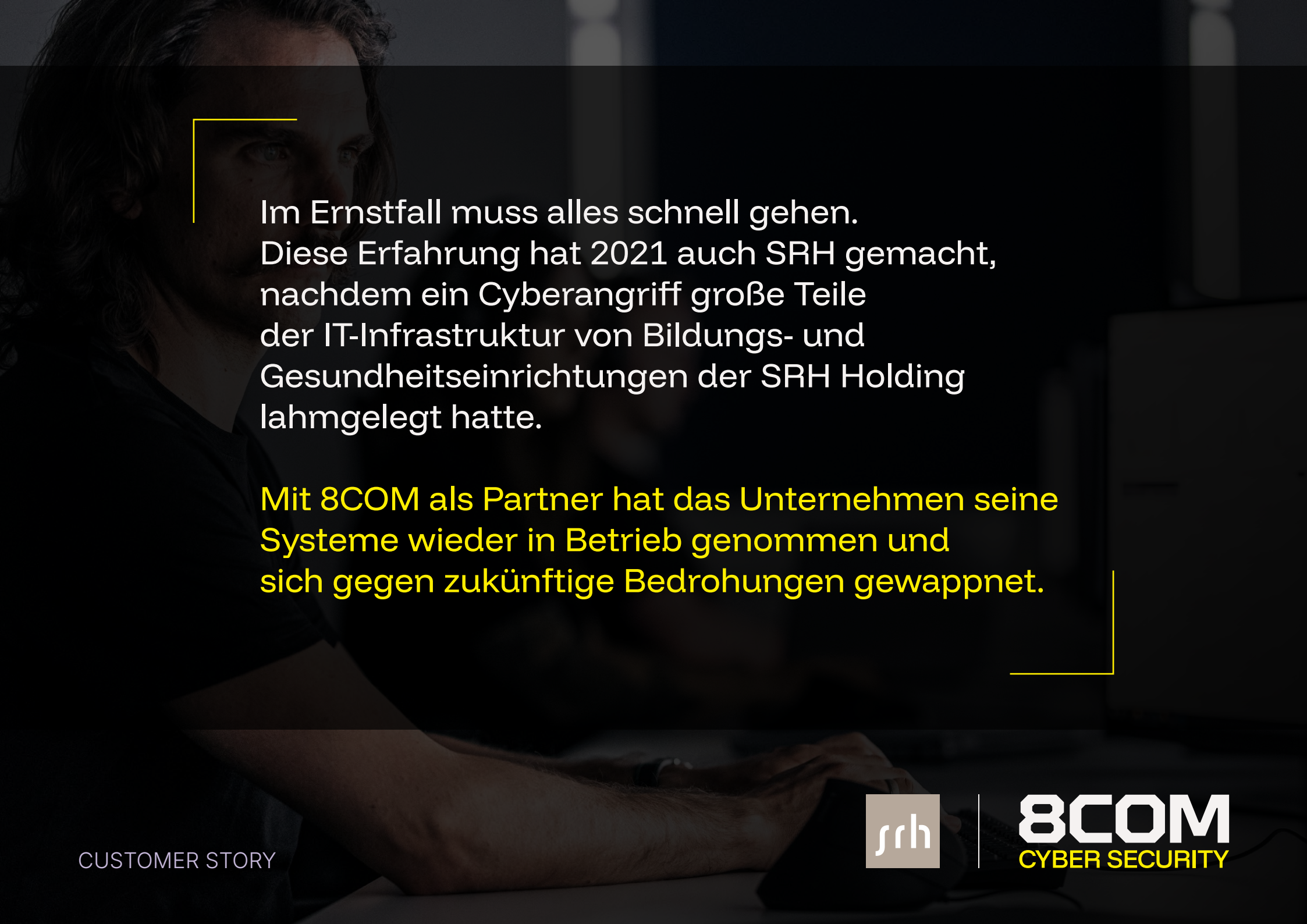
Nach dem Angriff ist vor dem Angriff:

Wie SRH mit dem 8COM SOC seine IT-Sicherheit neu aufgestellt hat

CUSTOMER STORY

srh | 8COM CYBER SECURITY



Im Ernstfall muss alles schnell gehen.
Diese Erfahrung hat 2021 auch SRH gemacht,
nachdem ein Cyberangriff große Teile
der IT-Infrastruktur von Bildungs- und
Gesundheitseinrichtungen der SRH Holding
lahmgelegt hatte.

Mit 8COM als Partner hat das Unternehmen seine
Systeme wieder in Betrieb genommen und
sich gegen zukünftige Bedrohungen gewappnet.

CUSTOMER STORY

srh | 8COM CYBER SECURITY

8COM SOC
Customer Story

SRH IT Solutions

Der Kunde

SRH IT Solutions bewirtschaftet die strategische und operative IT für bundesweit mehr als 50 Unternehmen, die zur SRH Holding gehören und insgesamt mehr als 17.000 Menschen beschäftigen. Das IT-Team von etwa 200 engagierten Mitarbeitenden betreibt von 17 Standorten aus zentrale Geschäftsapplikationen, betreut rund 2.000 Server und über 18.000 Endgeräte – und damit eine komplexe IT-Landschaft mit hohen Anforderungen an die Cybersicherheit.

Über 8COM

Seit 20 Jahren schützt 8COM Unternehmen und Behörden vor Cyberangriffen, inzwischen rund um die Uhr im Schichtbetrieb, direkt vor Ort in Deutschland. Aktuell sind 120 Mitarbeitende dafür verantwortlich, die Cyber-Resilienz von mehr als 115 Kunden in über 40 Ländern zu stärken. Die Kernprozesse des 8COM SOC sind nach BSI IT-Grundschutz zertifiziert.

8COM SOC
Customer Story

Der Vorfall: Ransomware-Angriff trifft Bildungseinrichtungen und Hochschulen

Der Cyberangriff auf Unternehmen der SRH Holding im September 2021 sorgte bundesweit für Schlagzeilen und hatte weitreichende Auswirkungen auf den Geschäftsbetrieb. Cyberkriminelle hatten Malware in die IT-Systeme eingeschleust, woraufhin zentrale Dienste wie E-Mail und Netzlaufwerke nicht mehr erreichbar waren.

Betroffen waren vor allem die Bildungs- und Hochschuleinrichtungen, doch auch zahlreiche Kliniken gerieten infolge des Angriffs unter Druck. Dort wurde der Betrieb auf Notfallabläufe umgestellt: Dokumentation und Organisation liefen zeitweise wieder analog mit Stift und Papier, digitale Routinen waren außer Kraft gesetzt. Die medizinische Versorgung der Patientinnen und Patienten war jedoch zu jedem Zeitpunkt sichergestellt.

Im Verlauf der Ermittlungen verdichteten sich die Hinweise auf einen Ransomware-Angriff: Die Täter versuchten, das Unternehmen zu erpressen und hatten Daten kopiert, von denen einige später im Darknet auftauchten. SRH ging nicht auf Lösegeldforderungen ein und informierte Polizei, Landeskriminalamt und Datenschutzbehörden.

Die Aufgabe von SRH IT Solutions bestand nun darin:

- den Vorfall aufzuklären,
- Systeme wiederherzustellen
- und die Sicherheitsarchitektur zu stärken, um optimal gegen zukünftige Angriffe gewappnet zu sein.

Die Herausforderungen

8COM unterstützte SRH IT Solutions bei der Bewältigung und Aufarbeitung des Vorfalls. Keine leichte Aufgabe, denn verschiedene Unternehmensbereiche und sehr große Teile der Infrastruktur waren von dem Cyberangriff betroffen.

Wiederherstellung und forensische Aufklärung

Interne IT-Teams arbeiteten gemeinsam mit 8COM und anderen externen Spezialisten daran, Systeme zu überprüfen, neu aufzusetzen und schrittweise wieder in Betrieb zu nehmen. Nach einem halben Jahr hatte sich der IT-Betrieb weitgehend stabilisiert.

Rund-um-die-Uhr-Überwachung der IT-Systeme

Nach einem Notfall-Onboarding wurden die IT-Systeme zügig an die SOC-Umgebung von 8COM angeschlossen. Heute überwacht das SOC für SRH IT Solutions eine breite Palette sicherheitsrelevanter Datenquellen.

SOC as a Service von 8COM: Maximaler Schutz, rund um die Uhr

Das 8COM SOC setzt auf erfahrene Analysten sowie leistungsstarke XDR- und SIEM-Plattformen, um die Kundensysteme – Firewalls, Active Directory, Microsoft 365, Entra ID und mehr – 24/7/365 zu überwachen. So kann sich das Team von SRH IT Solutions ganz auf das Tagesgeschäft konzentrieren.

Umfassende Überwachung

Verdächtige Aktivitäten und Alarme werden kontinuierlich analysiert, korreliert und priorisiert, sodass sicherheitsrelevante Ereignisse frühzeitig erkannt und zielgerichtet bearbeitet werden können.

Deutlich verkürzte Reaktionszeiten

Durch den Einsatz einer XDR-Plattform werden Bedrohungen schneller und umfassender erkannt und über SOAR-Playbooks standardisiert verarbeitet, was für kurze Reaktionszeiten sorgt.

Volle Transparenz über die Sicherheitslage

Der Austausch zwischen SRH und dem 8COM SOC erfolgt transparent über ein Ticketsystem, ergänzt durch monatliche Management-Reports und Echtzeit-Dashboards.

Kontinuierliche Verbesserung

Das SOC nutzt klar definierte KPIs wie False-Positive-Rate und MTTR, optimiert fortlaufend Regeln und Workflows und hält Technologie sowie Fachwissen durch regelmäßige Evaluierungen und Weiterbildungen auf dem neuesten Stand.

8COM SOC
Customer Story

Tipp für andere Unternehmen: Nicht warten, bis es zu spät ist

Ein verheerender Cyberangriff kann jedes Unternehmen treffen. Umso wichtiger sind Investitionen in die Absicherung von IT-Infrastrukturen. Ein erfolgreicher Cyberangriff kostet betroffene Betriebe nicht nur Zeit und Geld für die Wiederherstellung der Systeme, sondern kann auch deren Ruf und öffentliches Ansehen schädigen.

„Unternehmen sollten nicht einfach abwarten, bis etwas passiert", warnt Dr. Stefan Müller, CISO der SRH. „Verantwortliche sollten lieber jetzt schon versuchen, die finanziellen Ressourcen für ein SOC zu bekommen."

„Inmitten des Cyberangriffs stand uns das Expertenteam von 8COM sofort zur Seite. Ihre Unterstützung half uns, schnell wieder handlungsfähig zu werden und die Kontrolle über unsere IT-Systeme zurückzubekommen."

Dr. Stefan Müller | *Group-CISO*
SRH