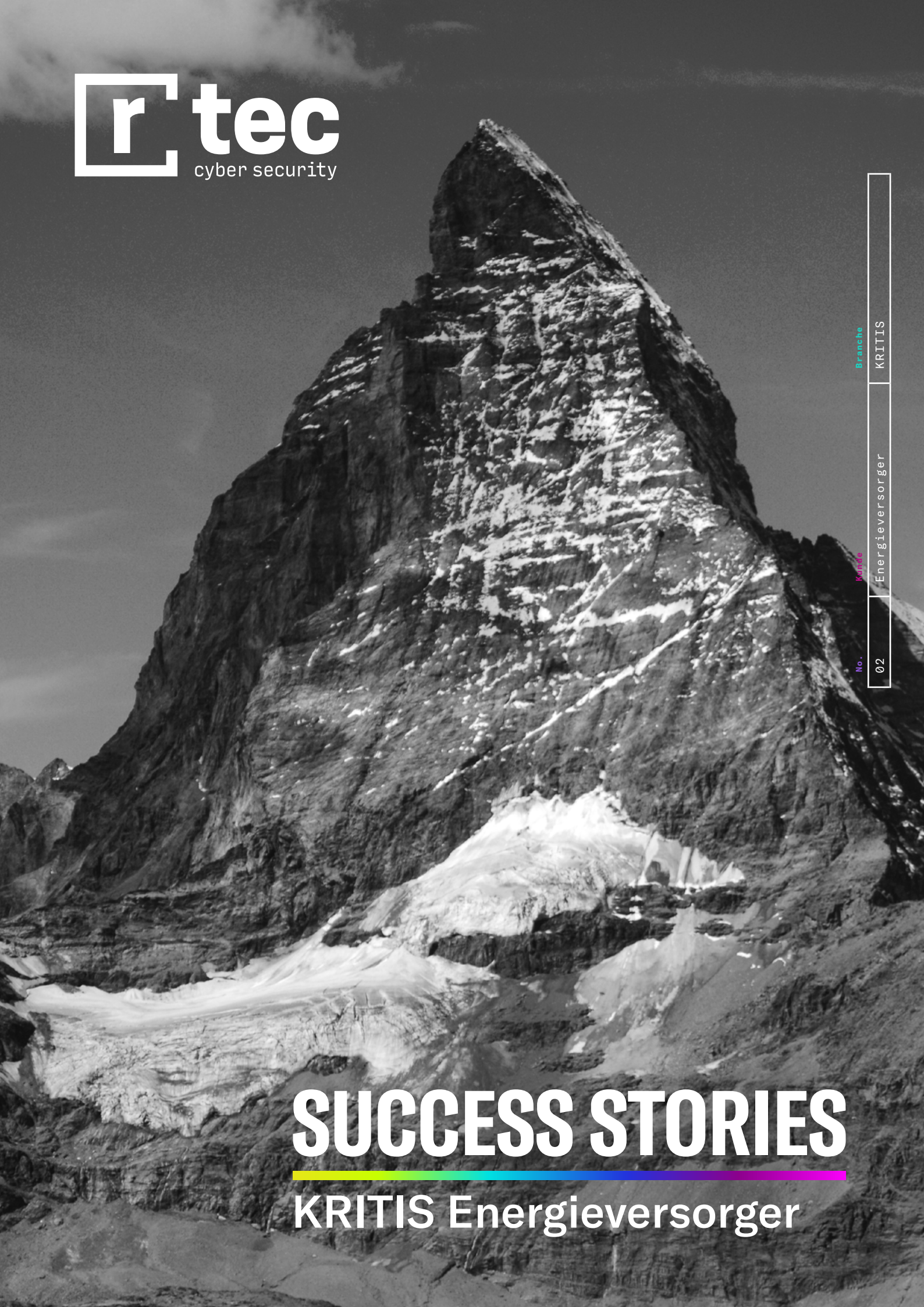

r tec
cyber security

Branche KRITIS

Kunde Energieversorger

No. 02

SUCCESS STORIES

KRITIS Energieversorger

KRITIS ENERGIEVERSORGER.

Schnelle Hilfe im Angriffsfall.

Alle Fakten auf einen Blick:

Aufgabe

- Untersuchung eines Cyberangriffs im Bereich kritischer Infrastrukturen
- Analyse von Web-, Internet-, DNS- und E-Mail-Kommunikation über einen langen, definierten Zeitraum
- Aktive Suche nach Indikatoren eines Angriffes
- Live-Untersuchung von ca. 2.500 Systemen
- Suche nach Anzeichen einer Kompromittierung in allen Office- und KRITIS-Bereichen ohne Beeinträchtigung des Betriebes
- Auswertung von Millionen Events

Vorgehen

- Implementierung von Sofortmaßnahmen
- Untersuchung aller relevanten Gateways und deren Protokolldaten, insbesondere Firewalls, Proxy- und DNS-Server, E-Mail-Daten, Security-Systeme
- Forensische Analyse eines verdächtigen Systems
- Planung des Rollouts der Analysesoftware für 2.500 Systeme
- Rollout der Analysesoftware in heterogenen Netzwerken und für Standby- und Offline-Systeme
- Analyse von 2.500 Systemen
- Manuelle Qualifizierung von ca. 20.000 kritischen Events
- Manuelle Detailuntersuchung verdächtiger Systeme

Projektziele

- Feststellung, ob Cyberangriff erfolgreich war
- Identifikation des Ausmaßes insbesondere der betroffenen KRITIS-Bereiche
- Identifikation und Bereinigung aller Spuren von Schadsoftware und sonstiger Anomalien
- Optimierung der Informationssicherheitsstrategie auf Basis der Erfahrungen aus dem Cyberangriff
- Definition zukünftig erforderlicher Cyber-Defense-Strategie

Ergebnisse

- Nachweis des Angriffsversuchs
- Verhinderung des Angriffs durch vorhandene Sicherheitsmaßnahmen
- Kein System – weder im Office- noch in den KRITIS-Bereichen – war durch Advanced Persistent Threats kompromittiert
- Identifikation aktiver Bedrohungen, u. a. trojanisierte Device-Treiber mit Keylogger oder Reste von Malware – auch auf Systemen in den KRITIS-Bereichen
- Definition der Ziele für eine wirksame, bereichsübergreifende Cyber-Defense-Strategie und Präsentation auf Vorstandsebene

Uns haben die professionelle Arbeit und die fachliche Qualifikation der Berater überzeugt. Wir haben uns jederzeit bei den Ansprechpartnern sicher aufgehoben gefühlt. Besonders gefallen hat uns die enge Einbindung und Schulung unserer Administratoren. Es war ein gutes Gefühl, dass unsere eigenen Leute ihre kritischen Systeme selbst scannen durften. Im Ergebnis eine ›runde Sache‹.

Kritische Infrastrukturen (KRITIS) sind „Organisationen und Einrichtungen mit wichtiger Bedeutung für das staatliche Gemeinwesen, bei deren Ausfall oder Beeinträchtigung nachhaltig wirkende Versorgungsengpässe, erhebliche Störungen der öffentlichen Sicherheit oder andere dramatische Folgen eintreten würden“ (BSI). Die zuverlässige Erbringung der kritischen Dienstleistungen bildet die Grundlage vieler alltäglicher Prozesse und Abläufe für die Bevölkerung und in der Wirtschaft. Sie ist Voraussetzung für die ausreichende Versorgung der Bevölkerung mit Lebensmitteln, Wasser, Elektrizität, Gesundheitsleistungen und vielen anderen wichtigen oder lebensnotwendigen Ressourcen. Vor diesem Hintergrund ist der Schutz Kritischer Infrastrukturen eine gesamtgesellschaftliche Aufgabe, die im Zusammenspiel von Staat, Wirtschaft und Öffentlichkeit erfolgt.

Wir haben uns auf den Schutz dieser Unternehmen und Anlagen spezialisiert.

Medienberichten zufolge mehren sich derzeit Sicherheitsvorfälle bei deutschen Energieversorgern. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) ist über diese Vorfälle informiert und hat diese in Zusammenarbeit mit dem betroffenen Unternehmen analysiert und bearbeitet. Hierzu erklärt BSI-Präsident Arne Schönbohm: „Die Anzahl und Qualität der Cyber-Angriffe nimmt zu, auch Betreiber Kritischer Infrastrukturen sind verstärkt im Fokus. Als nationale Cyber-Sicherheitsbehörde arbeiten wir intensiv mit der KRITIS-Wirtschaft zusammen, um Schutzmaßnahmen zu verbessern und Cyber-Angriffe abzuwehren.“

Ausgangspunkt des hier anonymisiert beschriebenen Projektes war der Angriff auf ein Energieversorgungsunternehmen. Die besondere Herausforderung bestand darin, in möglichst kurzer Zeit die erforderlichen Maßnahmen zur Aufklärung des Angriffs, Absicherung der betroffenen Systeme im laufenden Betrieb und damit Sicherstellung der weiteren Versorgung der Bevölkerung zu definieren und auszuführen.

Das vorrangige Ziel zu diesem Zeitpunkt: die Feststellung, ob der Cyberangriff erfolgreich war und gegebenenfalls in welchem Ausmaß das Unternehmen, insbesondere die „kritischen“ Bereiche betroffen waren, sowie die Unterbrechung der Kommunikationswege möglicher Angreifer.

Die geleistete Ersthilfe: die Implementierung von Sofortmaßnahmen zu Erkennung von Anomalien und eine umfassende forensische Analyse aller möglicherweise betroffenen Anlagen und Systeme, um das Ausmaß des Angriffs genauer zu bestimmen und eingrenzen zu können.

Innerhalb von fünf Arbeitstagen erfolgte die Live-Untersuchung von ca. 2.500 Systemen aus acht Unternehmensbereichen im laufenden Betrieb. Millionen erkannter Events mussten analysiert und ausgewertet werden. Im Ergebnis konnten ca. 20.000 kritische Events qualifiziert werden. Alle Spuren identifizierter Schadsoftware und sonstiger Anomalien konnten bereinigt werden.

Der Versuch eines Cyberangriffes konnte forensisch nachgewiesen werden. Der Angriff wurde jedoch nachweislich durch die vorhandenen Sicherheitsmaßnahmen wirksam verhindert. Kein System – weder im Office- noch in den KRITIS-Bereichen – war durch Advanced Persistent Threats kompromittiert.

Für die Zukunft konnten wesentliche Ziele für eine wirksame, bereichsübergreifende Cyber-Defense-Strategie ermittelt und auf Vorstandsebene präsentiert werden. Nächster Schritt der Zusammenarbeit ist ein Workshop zum Abgleich der vorhandenen Sicherheitsarchitektur mit einem von r-tec zu erstellenden optimierten Sicherheitsarchitekturentwurf. ■

Die r-tec IT Security GmbH, mit Sitz in Wuppertal, wurde 1996 von Dr. Stefan Rummenhöller gegründet. Als Wegbereiter und Wegbegleiter schaffen wir für unsere Kunden sichere Räume für die Entwicklung ihrer Organisationen und die Verwirklichung ihrer Visionen. Unsere Kunden aus dem gehobenen Mittelstand, Konzerne, kommunale Rechenzentren und Bundes- oder Landesbehörden vertrauen seit über 20 Jahren auf unsere hoch spezialisierten Experten.

Als Strategic Supplier für Cyber Security Services schützen wir die Werte unserer Kunden vor Bedrohungen und begleiten ihr Security Management von der Initiierung über die Einführung bis zum Betrieb auf allen Ebenen.

Wir leben Regeltreue, höchste Qualitätsstandards und Servicementalität. Unser Unternehmen haben wir nach den Strukturen und Richtlinien der DIN ISO 9001:2015 und der ITIL aufgebaut. Wir sind nach ISO 27001 zertifiziert.

r-tec IT Security GmbH | Hatzfelder Str. 167 | 42281 Wuppertal
www.r-tec.net | +49 (0) 202 31767–100