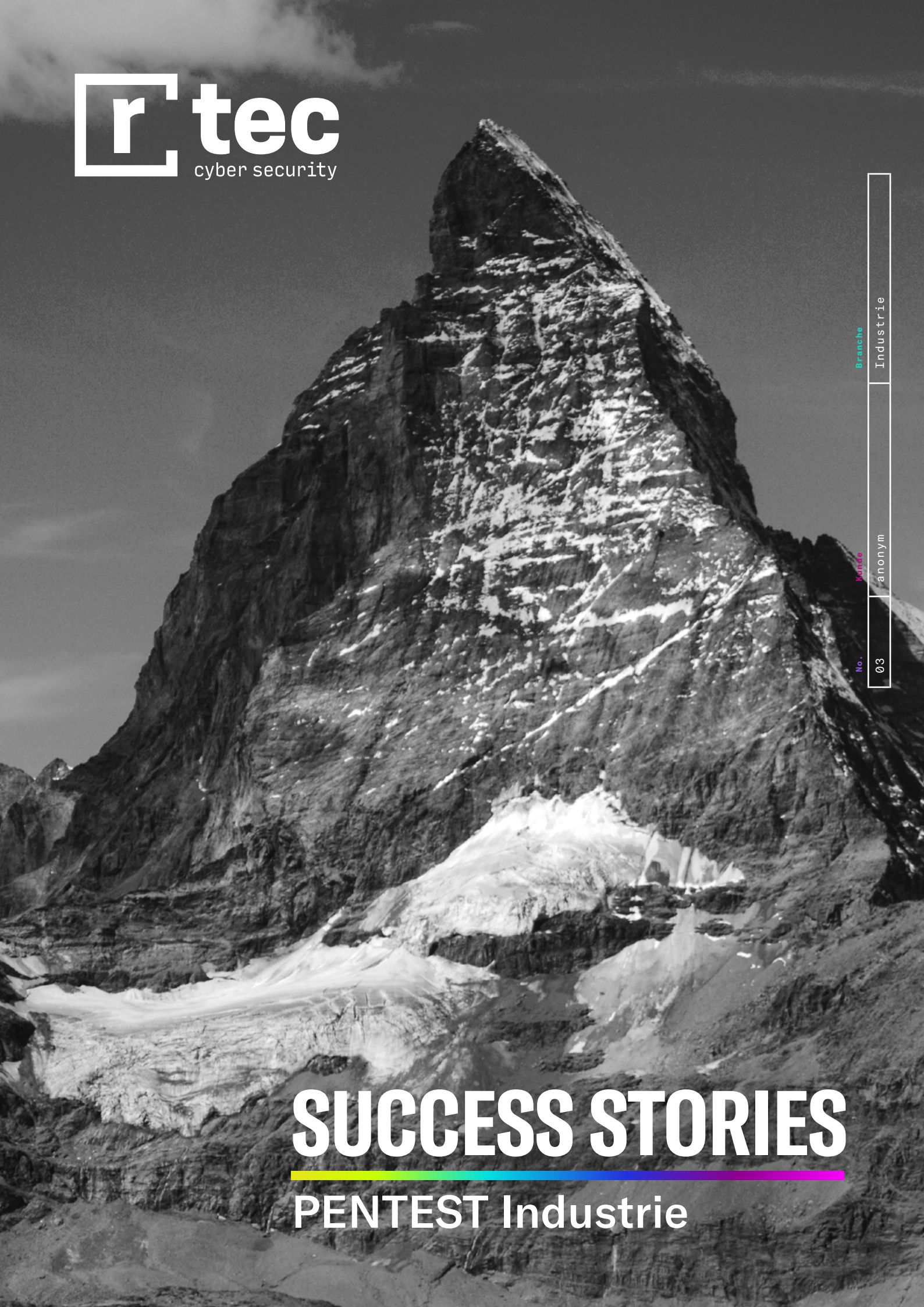

r tec
cyber security

Branche
Industrie

Kunde
anonym

No.
03

SUCCESS STORIES

PENTEST Industrie

PENTEST INDUSTRIE.

Licht ins Dunkel bringen.

Alle Fakten auf einen Blick:

Aufgabe

- Analyse von Active Directory (AD), SAP-Landschaft, Azure Cloud
- Aktive Suche nach Einfallstoren, die Zugriff auf die Windows-Arbeitsplätze, Storage-Server, SAP-Systeme, E-Mail und SharePoint ermöglichen

Vorgehen

- Angriffe auf das lokale AD aus Sicht eines internen Angreifers
- Schwachstellen-Scan der Infrastruktur aus dem Client-Netzwerk (LAN)
- Angriffe auf Clients im Betrieb

Projektziele

- Identifikation potenzieller Schwachstellen
- Bewertung des Gefährdungspotenzials und der Kritikalität
- Einstufung des Sicherheitsniveaus
- Offenlegung von Verbesserungspotenzial
- Erarbeitung eines Maßnahmenkatalogs

Ergebnisse

- Innerhalb von 45 Minuten konnten administrative Rechte im AD erlangt werden
- Am gleichen Tag konnte Vollzugriff auf die Cloud-Dienste erlangt werden (Azure AD)
- Root-Rechte auf die komplette SAP-Landschaft
- Stille Umgehung der Firewall
- Zugriff auf alle Unternehmensdaten: Clients, E-Mails, SAP-Datenbanken

Wir waren überrascht über das Ausmaß der vorhandenen Sicherheitslücken und die daraus entstehenden Möglichkeiten für Angreifer, an relevante Informationen und Daten heranzukommen und kritische Systeme zu übernehmen. Wir wissen nun, welche insbesondere auch strukturellen Verbesserungen wir vornehmen müssen.«

Der Pentest als Ausgangspunkt zur Verbesserung des Sicherheitsniveaus

»Illegaler Wissens- und Technologietransfer, Social Engineering und Wirtschaftssabotage sind keine Einzelfälle, sondern ein Massenphänomen.« Kunden- und Finanzdaten, Patente, F&E-Ergebnisse und insbesondere Kommunikationsdaten wie E-Mails werden regelmäßig durch eine heterogene Täterschaft zwecks Erpressung, Wirtschaftsspionage oder Sabotage gestohlen, so der Bundesverfassungsschutz-Präsident Thomas Haldenwang.

Der Auftraggeber des hier anonymisiert beschriebenen Projektes ist beispielhaft für ein verwundbares Unternehmen, denn in den vergangenen zwei Jahren wurden 7 von 10 Industrieunternehmen Opfer von Sabotage, Spionage oder Datendiebstahl. Das Projekt aus dem Jahr 2018 wurde bei einem großen deutschen Industriekonzern ausgeführt. Als Projektziel wurden die Überprüfung der Firmennetzwerke, die Übernahme der Systeme und die Prüfung des Zugriffs auf sensible Daten definiert.

Bei der Überprüfung auf potenzielle Schwachstellen konnten unsere Spezialisten die höchsten Rechte im lokalen »Active Directory«, dem Quasi-Industriestandard für Verzeichnisdienste, übernehmen – und das innerhalb einer Stunde. Am ersten Projekttag konnte Vollzugriff auf das Cloud-Verzeichnis realisiert werden, sodass nicht nur der Betrieb, sondern auch der gesamte Konzern hätte kompromittiert werden können.

Die intern feststellbare Problematik: Es wurden die gleichen Zugangsdaten in der Cloud benutzt, die auch auf den lokalen Rechnern verwendet wurden. Die IT-Administratoren nutzten teilweise keine Zwei-Faktor-Authentifizierung, obwohl dies bereits Industriestandard ist. Die r-tec-Profis konnten alle E-Mails einsehen und jede beliebige Datei aller Windows-Systeme auslesen.

In Absprache mit dem Kunden wurden die relevanten Abteilungen nicht über die Penetrationstests informiert, um eine möglichst realitätsnahe Wirkung zu simulieren. Die Firewall des Auftraggebers griff zunächst ein und verwarf diverse Eintrittsversuche; die r-tec-Experten konnten jedoch mit den zuvor ausgelesenen Zugangsdaten die Firewall deaktivieren und ungestört weiter vordringen. Die über einen längeren Zeitraum andauernden und erfolgreichen Angriffe blieben von den Fachabteilungen unentdeckt.

Neben Windows-Servern und -Clients konnte auch die SAP-Landschaft erfolgreich angegriffen werden. Bereits bekannte Schwachstellen konnten ausgenutzt werden – wiederkehrende Passwörter und die Fehlkonfiguration infolge eines nicht ausreichenden Sicherheitsbewusstseins ermöglichten die Rechteerhöhung und Vollzugriff auf die Business Intelligence Datenbank SAP-HANA.

Im Ergebnis konnte dem Auftraggeber eine Liste mit veralteten Versionsständen von Servern und Clients, kritischen Active-Directory-Schwachstellen und nicht geänderter Standardzugangsdaten übergeben werden.

Für die zukünftige Zusammenarbeit wurden weitere Maßnahmen vereinbart. Um substanziellen Schwächen der Sicherheitsstruktur auf den Grund zu gehen, wird ein Architekturreview durchgeführt. Bis zur Erreichung des angestrebten Sicherheitsniveaus werden die Penetrationstests monatlich wiederholt, damit der Fortschritt der Maßnahmenintegration festgehalten werden kann. Schließlich wird mit einem Abonnement des r-tec Schwachstellen-Scan-Service sichergestellt, dass auch in der Zukunft Sicherheitslücken nicht im Verborgenen bleiben. ■

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