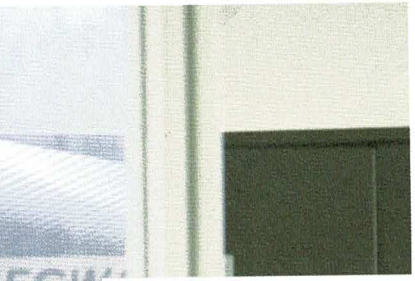


Besonders schutzbedürftig: das Rechenzentrum, über das alle IT-Aktivitäten des Konzerns weltweit laufen.

GEHEIMWAFFE AUFMERKSAMKEIT

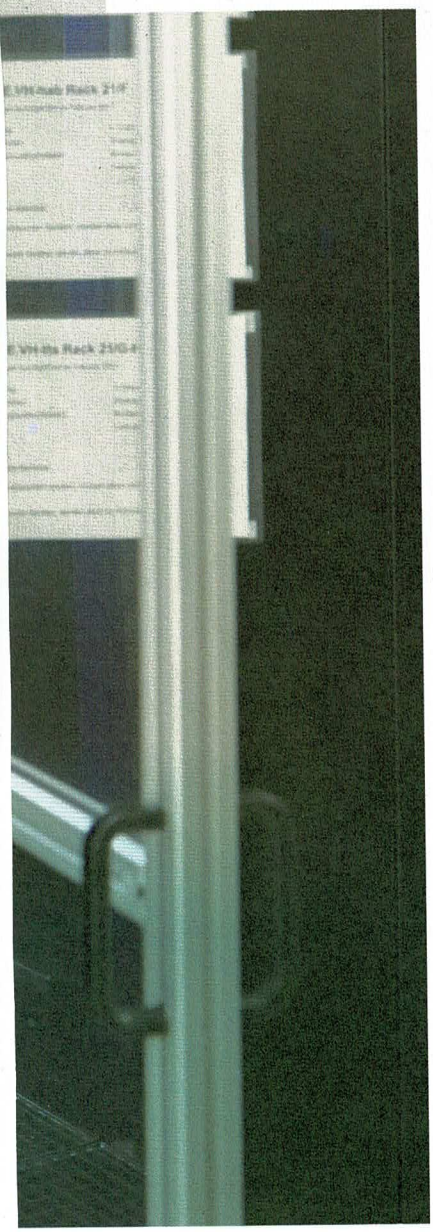


Foto: Ralf Baumgarten

Zu den Erfolgsfaktoren des Spezialistenteams für Cybersecurity der Voith Group in Heidenheim zählen: Anomalien im Datenverkehr aufzuspüren und die Aufmerksamkeit der Mitarbeiter für Cybersecurity zu erhöhen. Das Reporterteam des VDMA-Magazins erhielt exklusive Einblicke.

AUTOR: NIKOLAUS FECHT

Die Spurensuche beginnt mitten in Heidenheim an der Brenz im Osten Baden Württembergs an der Grenze zu Bayern: Oben auf dem Felsen lockt unübersehbar das mittelalterliche Schloss Hellenstein, das Wahrzeichen Heidenheims. Unten im Tal befindet sich das Voith Training Center in einem fünfstöckigen Bürokomplex. Alles strahlt die kreative Nüchternheit des erfolgreichen Hightech-Konzerns Voith aus, der mit weltweit mehr als 19 000 Mitarbeitern Anlagen, Produkte, Serviceleistungen und digitale Anwendungen anbietet.

Im obersten Stock wartet bereits Rolf Strehle. „Das ist einer der altgedienten Cybersecurity-Pioniere der Branche", hatte uns Steffen Zimmermann, Leiter Competence Center Industrial Security beim VDMA, mit auf den Weg gegeben. Strehle ist Leiter des Competence-Centers IT-Sicherheit bei Voith.

Der jugendlich wirkende Mann nimmt im überdimensionalen Sessel Platz: Rund zehn Meter schräg unter uns trainieren Azubis an Maschinen, über ihnen, einen Stock höher, lernen Voith-Mitarbeiter den Umgang mit neuer Software. Zu den Gästen zählen auch IT-Experten des Konzerns aus aller Welt, die Voith zu Trainern für Cyberresilienz, der neuen Aufmerksamkeit im Umgang mit IT und Vernetzung, ausbildet.

Cyberresilienz: Awareness fördern

Die Schulung verdanken sie einem unschönen Erlebnis im Jahr 2014. „Wir überprüften als Hacker mit Erlaubnis der Geschäftsleitung, wie viele unserer Systeme angreifbar sind", runzelt Strehle bei der Erinnerung an den Vorfall die Stirn. „Von insgesamt 25 000 waren es im ersten Anlauf bereits 200. Wir stießen auf sehr viele PCs, Tablets und Smartphones." Da setzte ein Umdenken bei Voith ein. Der Cybersecurity-Pionier beugt sich nach vorne und signalisiert mit offenen Händen den neuen Weg: „Wir starteten mit Erfolg eine Awareness-Kampagne, dank der mittlerweile jeder Mitarbeiter weltweit einmal pro Jahr eine Schulung ▸

zur Informationssicherheit erhalten muss. Vermittelt wird etwa: Passt auf, wenn ihr ein Handy oder Notebook im Betrieb nutzt!" Die Schulung geschieht zweigleisig per E-Learning am Arbeitsplatz und durch die selbst ausgebildeten Cyberresilienz-Auditoren.

Besonders schützen müssen Strehles Experten vor allem das Rechenzentrum, über das alle IT-Aktivitäten des Konzerns weltweit laufen. Zutritt in diesen streng geschützten Bereich ermöglicht uns Andreas Weidner. Er trägt als Senior Manager Information Security Officer (CISO) die Gesamtverantwortung für die Informationssicherheit bei Voith. Weidner führt uns über eine geschwungene Brücke über das Flüsschen Brenz („Damit kühlen wir unsere Rechner") zu einem alten Fabrikgebäude aus den 50er-Jahren, dessen Treppenhaus an den früheren Stil aus der Zeit des deutschen Wirtschaftswunders erinnert.

„Unser Anomalie-Detektion-System entdeckt frühzeitig, wenn im Netz etwas nicht stimmt."

ROLF STREHLE

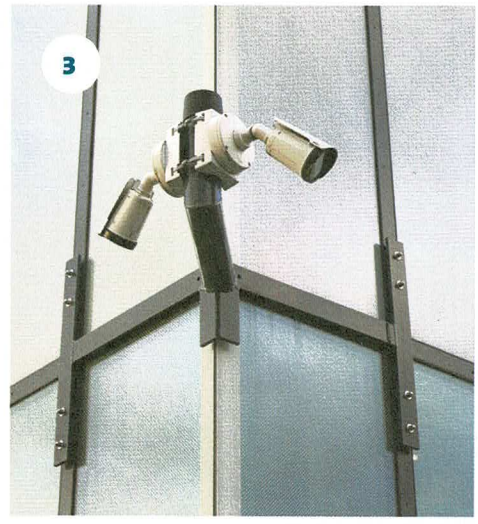
Im Keller begrüßt uns Helmut Reiter, der als Senior Manager IT Infrastructure Zutritt zum Allerheiligsten hat: Der Diplomphysiker öffnet die Tür mithilfe eines Fingerprint-Sensors. Beim Eintreten des Raums umhüllt uns gleich die warme Abluft aus den laut brummenden Kühlern der Server, die auch als Cloud für den Konzern dienen. In den großen weiß-grauen Kästen steckt die Speicherkapazität von 30 000 Terabyte – genug, um die Daten von 50 000 Laptops zu speichern. Zudem existiert nicht weit entfernt ein zweites Rechenzentrum, das alle Daten permanent spiegelt und im Falle eines Ausfalls einspringen kann.

Die IT-Experten merken schon, dass sich die Einstellung zu ihnen und zur IT-Security gewandelt hat. „Die Awareness ist gestiegen", bestätigt uns Physiker Reiter wegen des Lärms im Rechenzentrum mit lauter Stimme. „Wir spüren das neue Bewusstsein heute bei jedem Mitarbeiter. Aufgerüttelt hat sie Strehles Awareness-Kampagne, aber auch die vielen Presseberichte über Cyberangriffe."

1 — Rolf Strehle zählt zu den altgedienten Cybersecurity-Pionieren der Branche.

2 — Das Voith Training Center schult Azubis und bildet auch IT-Experten zu Trainern für Cyberresilienz aus.

3 — Die Überwachung des Geländes per Kameras schützt vor unerwünschten Besuchern.



Gezielte Suche nach Anomalien

Doch Awareness allein reicht nicht aus, nötig sind auch Wächter mit dem Gespür für mögliche Cyberangriffe. Viele Mitarbeiter aus Strehles Mannschaft haben deswegen eine Spezialausbildung zum legalen Hacken absolviert. Sie sitzen außerhalb des Voith-Werksgeländes in gemieteten Büroräumen. „Eine unserer Spezialitäten ist die gezielte Suche nach Anomalien im Datenverkehr", erklärt der Geschäftsführer, während er mit uns in seinem Wagen zum nahegelegenen Kompetenz-Zentrum fährt. „Im Kreditverkehr

4 ___ In den Serverschränken des gut gesicherten Rechenzentrums steckt die Speicherkapazität von 30 000 Terabyte.

5 ___ Die Mitarbeiter im Kompetenz-Center überwachen im Kundenauftrag Anomalien im Datenstrom.

Fotos: Ralf Baumgarten

gibt es das schon lange. Wenn Sie heute in China eine Kreditkarte aktivieren und dies kurz darauf auch in Deutschland tun, dann sperrt sie das Kreditkarteninstitut sofort." Weil es das in der IT nicht gab, habe er mit seinem Team ein System entwickelt, das den Konzern bereits mehrmals vor ernsthaften Attacken gerettet hat.

Ging es da auch um den WannaCry-Virus, der im Jahr 2017 Daten verschlüsselt hat und so viele Unternehmen lahmlegte? „Ja, er bedrohte die Produktion, griff dort an, wo es richtig weh tut", verrät Strehle ernst blickend. Lächelnd fährt er fort: „Doch lange bevor alle IT-Schutzeinrichtungen wie Firewall oder Virenscanner aktiv wurden, schlug die Stunde unseres Anomalie-Detektion-Systems. Es entdeckte frühzeitig, dass im Netz etwas nicht stimmt." Alarmiert vom System spürten die Spezialisten des Kompetenz-Zentrums den Virus noch am selben Tag auf und verhinderten so einen verheerenden Angriff auf die insgesamt 40 000 Rechner der weltweiten Produktion.

Firmeneigene Hacker

Diese firmeneigenen Hacker müssen wir kennenlernen! Neugierig steigen wir am Rand der Stadt aus Strehles Auto aus und stehen vor einem grauen, unscheinbaren dreistöckigen Bürogebäude. Im ersten Stock befindet sich das Kompetenz-Center, laut Voith einer der größten ▸

SHORT FACTS

60 %

der Maschinenbauer gehen davon aus, .dass die Zahl der Sicherheitsvorfälle zunehmen wird.

Am

11.03.2020

thematisiert der Cybersecurity-Kongress von VDW und VDMA in Düsseldorf das Zusammenwachsen von Office- und Produktionswelt.

ISO/IEC 27001

heißt das Zertifikat, das einem Unternehmen die Überprüfung aller sicherheitskritischen Prozesse und Systeme seines Rechenzentrums attestiert.

6 — Andreas Weidner (rechts) verantwortet die Informationssicherheit bei Voith.

7 — Akribische Ordnung bei der Verkabelung kennzeichnet eine gut gesicherte IT-Abteilung.

Security- und Datenschutzanbieter in Deutschland.

Es herrscht in den leicht abgedunkelten Räumen angespannte Ruhe, manche hören Musik über Kopfhörer, nur wenige sprechen leise miteinander. Peter Lorenz, ein rund 30-jähriger Experte, unterbricht seine Arbeit für Fotoshooting und Kurzinterview. „Ja, die Aufmerksamkeit der Voith-Mitarbeiter hat deutlich zugenommen", bestätigt uns der System Engineer. „Doch leider haben sich auch die Hacker darauf eingestellt: Die Cyberangriffe fallen immer kreativer aus." System Engineer Timo Kovacs kommt hinzu und bestätigt die Aussagen seines Kollegen. Und wer beschäftigt sich hier mit der Anomalie-Detektion? Lorenz deutet hinter die Stellage: „Der Kollege nebenan arbeitet gerade für einen Kunden an einem wichtigen Fall, aber bitte nicht stören!"

„Wir lernen von dieser Arbeit sehr viel, denn dank dem Feedback und dem ständigen Blick über den Tellerrand können wir unsere Werkzeuge – wie etwa den Anomalie-Detektor – neu justieren und verbessern", erklärt uns Strehle auf der Rückfahrt zur Konzernzentrale.

Diese ständige Weiterentwicklung sei sehr wichtig, denn wegen der zunehmenden Vernetzung im Rahmen von Industrie 4.0 drohen neue Gefahrenquellen. Oft stecke in einer neu gekauften Werkbank veraltete PC-Technik, die von sich aus unsicher sei. Strehles Plädoyer: „Unsere Industrie muss ihre Maschinen und Anlagen unter dem Stichwort ‚Security by Design' sicherer machen. Ein Anfang wäre etwa der virtuelle Sicherheitsschalter, der sich nicht hacken lässt." Und auf diesem Weg befindet sich gerade Voith bei seinen Maschinen und Anlagen – wahrscheinlich wieder als Pionier.

Steffen Zimmermann
Telefon +49 69 6603-1978
steffen.zimmermann@vdma.org

Veranstaltung
Security by Design am
30. März 2020 in Karlsruhe
go.vdma.org/c15qv

Competence Center im VDMA
industrialsecurity.vdma.org

„Für sicherheitskritische Funktionen ist eine zusätzliche Authentifizierung nötig."

PROF. DR. ERIC BODDEN

Direktor und Professor unter anderem für IT-Sicherheit am Fraunhofer-Institut für Entwurfstechnik Mechatronik IEM und am Heinz Nixdorf Institut der Universität Paderborn

„Die übergreifende Normenreihe IEC 62443 bietet Orientierungshilfe. Sie empfiehlt Steuerungsherstellern etwa einen relativ stringenten Entwicklungsprozess, der Security von Anfang an beachtet.

So sollten sich sicherkritische Funktionen nicht ohne eine zusätzliche Authentifizierung durchführen lassen. Maschinenbauer können in der Normenreihe nachlesen, wie sie sichere Komponenten auswählen und diese dann zu einer sicheren Anlage vereinen. Wichtig ist die Kommunikation zwischen den einzelnen Maschinenkomponenten, bei der jede Komponente unterscheiden sollte, von wem eine Anfrage kommt. Hier bietet sich die Kommunikation über offene Schnittstellen wie OPC UA an. Unterstützung bieten die gemeinsamen Schulungen des Fraunhofer IEM und des Maschinenbau-Instituts des VDMA.

Fotos: Ralf Baumgarten, Uni Paderborn