„Die Zukunft ist dezentral“

Interview mit Raphael Vallazza, Founder & CEO von Endian

Die Digitalisierung birgt für Unternehmen große Chancen, aber auch zahlreiche Gefahren. Das sieht die EU genauso und will den digitalen Risiken mit ihrer neuen Richtlinie NIS-2 entgegenwirken. Raphael Vallazza ist Geschäftsführer des Südtiroler Unternehmens Endian, das sich auf Lösungen für die Cybersicherheit spezialisiert hat. Im Interview erklärt er, welche virtuelle Bedrohungen es für die Gasbranche gibt, wie die EU sie mit NIS-2 davor schützen will und was sein Unternehmen tut, um Betriebe „NIS-2 ready“ zu machen.

gwf: Herr Vallazza, vor welchen Gefahren stehen Betreiber von Gasinfrastrukturen angesichts der Digitalisierung?
Raphael Vallazza: Eine große Herausforderung ist sicher, dass ihre Infrastrukturen dezentral aufgebaut sind. Trotzdem müssen sie zentral überwacht werden.

gwf: Wie gelingt das?
Vallazza: Die einzige Möglichkeit ist, seine Anlagen sauber zu vernetzen und sämtliche Aktivitäten zu monitoren. Andernfalls lässt sich die Frage, ob ein Netzwerk sicher ist, eigentlich gar nicht beantworten.

gwf: Wie erfolgt eine solche Vernetzung?
Vallazza: Ein wichtiges Element sind Security Gateways. Sie stellen sicher, dass nur authentifizierte Nutzer Zugang zum Netz haben. Auch eine lückenlose Protokollierung ist essentiell, die zeigt, was jemand wann und wo im Netz getan hat. Bevor Security Gateways und Protokollierung zum Einsatz kommen können, muss aber eine gewisse Vorarbeit geleistet werden. Wir haben die Erfahrung gemacht, dass viele Unternehmen gar nicht genau wissen, welche Komponenten in ihren Systemen im Einsatz sind.

(Quelle: Endian)

RAPHAEL VALLAZZA

ist seit 2003 Gründer und CEO von Endian

gwf: Wie kann das sein?
Vallazza: Es handelt sich meist um sehr komplexe und dynamische Netzwerke. Es ist daher nicht trivial, sämtliche Komponenten eines Systems aus tausenden oder zehntausenden Einzelteilen im Detail zu kennen. Eigentlich müsste man das nämlich, um die Sicherheit des Gesamtsystems evaluieren zu können. Hinzukommt, dass Maschinen grundsätzlich nicht für Cybersecurity konzipiert wurden und daher fast immer sehr unsicher sind.

gwf: Sie spielen auf den Unterschied zwischen „Safety“ und „Security“ an.
Vallazza: Genau. Natürlich müssen Maschinen hohe Sicherheitsstandards erfüllen, beispielsweise dürfen sie nicht explodieren oder anderen Schaden anrichten. Dazu hat die EU im Jahr 2006 umfangreiche Richtlinien veröffentlicht. Damals war Cybersecurity nur in der Informationstechnolgie (IT) ein Thema, in der OT aber noch nicht.

gwf: Was ist der Unterschied zwischen OT und IT?
Vallazza: Kurz gesagt: Betriebstechnologie (OT) steuert Geräte und IT steuert Daten. Wir haben schon vor über zehn Jahren mit der Entwicklung dezentraler Architekturen für die OT begonnen. Unsere Frage war, ob es möglich ist, tausende von Anlagen miteinander zu vernetzen, um sie vor digitalen Angriffen zu schützen. Das war damals noch unüblich, heute kommt Bewegung in das Thema.

gwf: Die EU will Unternehmen mit NIS-2 dazu verpflichten, sich stärker um die digitale Sicherheit ihrer Anlagen zu kümmern. Was genau hat es damit auf sich?
Vallazza: NIS-2 ist eine EU-Richtlinie, die die EU-Mitgliedsstaaten bis Oktober 2024 in nationale Gesetze überführen müssen. NIS-2 legt neue Standards für Cybersecurity fest. Wer die Regularien nicht einhält, muss nach einer gewissen Übergangsfrist empfindliche Strafen zahlen. Damit reagiert die EU auf die teils gravierenden Sicherheitslücken bei Unternehmen. NIS-2 ist übrigens Teil einer größeren EU-Initiative zu

dem Thema: 2027 tritt u. a. der Cyber Resilience Act (CRA) in Kraft, der hohe Sicherheitsanforderungen für jegliche Art von Software festlegt – auch für solche, die auf Maschinen läuft. Und heutzutage ist fast jede Maschine softwaregetrieben.

gwf: Sind die NIS-Standards sinnvoll?
Vallazza: Ich denke schon. Leider lassen viele Unternehmen die Cybersicherheit ihrer Anlagen schleifen, bis etwas passiert. Und es passiert häufiger etwas, als man denkt – viele erfolgreiche Cyberangriffe gelangen nicht an die Öffentlichkeit, weil es für die Unternehmen keine Meldepflicht gibt. Das soll sich mit NIS-2 ändern: Sämtliche Fälle von Cyber-Kriminalität müssen dann der EU weitergegeben werden.

gwf: Was genau kann denn „passieren"?
Vallazza: Maschinen lassen sich so manipulieren, dass sie kaputt gehen und dann explodieren oder zum Stillstand kommen. Natürlich kommunizieren Unternehmen solche Schwachstellen nicht gerne, aber in Gesprächen haben wir schon verheerende DInge gehört. Cyberangriffe sind zudem ein Teil der modernen Kriegsführung geworden. Sie sind deutlich günstiger als physische Angriffe, können aber enormen Schaden anrichten. Denken sie an ein Gaskraftwerk: Wenn es lahmgelegt wird und der Strom ausfällt, funktioniert die lokale Infrastruktur nicht mehr.

INFOKASTEN ZU NIS-2

Mit der NIS-2-Richtlinie gelten für Unternehmen und Organisationen in 18 kritischen Sektoren bald neue Sicherheitsmaßnahmen und Meldepflichten. NIS-2 ersetzt die NIS Directive von 2016 und soll das Niveau der Cybersicherheit in der EU verbessern und vereinheitlichen. Im Vergleich zur alten NIS Directive erweitert NIS-2 den Kreis den Kreis der betroffenen Unternehmen, ihre Pflichten und die behördliche Aufsicht erheblich. Bei Verstößen drohen hohe Geldstrafen.

gwf: Wie weit ist Deutschland damit, die Verordnung in nationale Gesetze zu gießen?
Vallazza: Das Bundeskabinett hat am 24. Juli den Gesetzentwurf zur Umsetzung in deutsches Recht verabschiedet. Zukünftig wird die Wirtschaft das NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz (NIS2UmsuCG) des Bundes einhalten müssen. Eine Umsetzung der Richtlinie bis zum 18. Oktober 2024 – wie von der EU geplant – ist nach aktuellem Stand eher unwahrscheinlich. Aber der CRA gilt definitiv ab 2027, und es ist erklärtes Ziel der EU, ab dann jene Unternehmen zu sanktionieren, die die Vorschriften nicht einhalten.

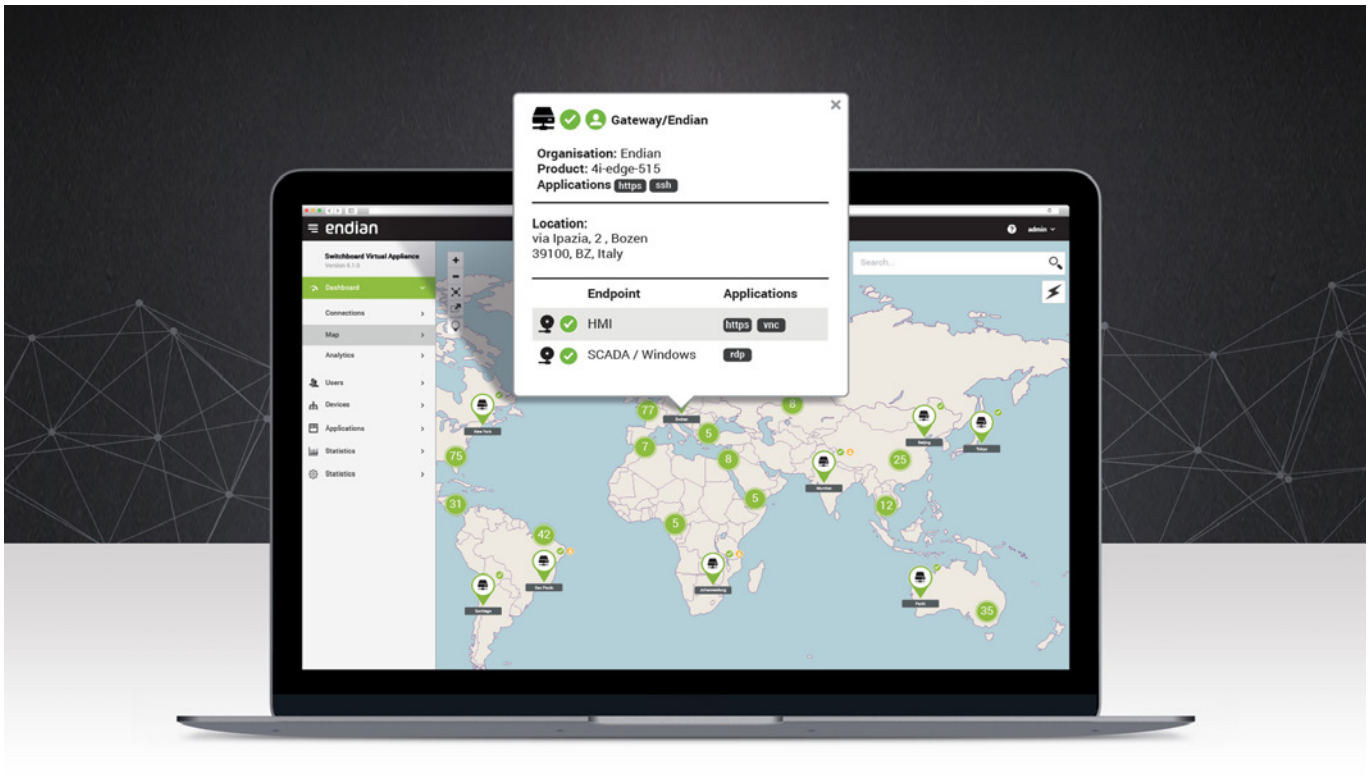
„Ohne Digitalisierung kein Wasserstoff – und ohne Cybersecurity keine Digitalisierung"

gwf: Bislang herrschte in puncto Cybersicherheit also „Wilder Westen".
Vallazza: Das kann man so sagen – den Unternehmen war es selbst überlassen, ob und wie sie sich vor Hackerangriffen schützen. Inzwischen hat der Gesetzgeber – auch durch die Corona-Pandemie – erkannt, wie verflochten die internationalen Produktionsketten sind. Jedes unzureichend abgesicherte Glied ist ein potenzielles Risiko. Für Unternehmen im Energiesektor gilt das natürlich im besonderen Maße.

gwf: Müssen sich alle Unternehmen im Energiesektor mit NIS-2 auseinandersetzen?
Vallazza: Fast alle. Das Interessante an NIS-2 ist der extrem große Scope: Alle Betriebe ab 50 Mitarbeitern und 10 Mio. € Jahresumsatz fallen unter die Richtlinie, also auch viele kleine und mittelständische Unternehmen. Leider hat die EU keinen einheitlichen Sicherheitsstandard festgelegt, sondern nur bestimmte Kriterien genannt – die technische Umsetzung bleibt den Staaten überlassen. Wir sind gespannt, wie das funktionieren wird.

gwf: Wer kontrolliert eigentlich die Einhaltung der Vorschriften?
Vallazza: Das Bundesamt für Sicherheit in der Informationstechnik (BSI). NIS-2 besagt, dass jedes Land eine eigene Cybersecurity-Behörde einrichten soll. Deutschland ist da mit dem BSI weiter als andere Länder. Alle Unternehmen müssen nach Inkrafttreten der neuen Gesetze ihre relevanten Vorfälle an das BSI melden. Von dort werden die Zahlen an die EU weitergegeben, die sie anonymisiert veröffentlicht. Spätestens dann werden alle verstehen, wie kritisch das Thema wirklich ist. Heute zahlen die meisten Unternehmen ein Lösegeld an die Hacker, wodurch die tatsächliche Zahl der Fälle im Dunkeln bleibt.

gwf: Inwiefern spielt NIS-2 eine Rolle für Ihr Unternehmen?
Vallazza: Der Umgang mit NIS-2 teilt sich in einen technischen und einen organisatorischen Bereich. Auf der organisatorischen Ebene müssen Unternehmen ihr Personal beim Thema Cybersicherheit schulen und definieren, wer bei einem



Quelle: Endian

Endian Switchboard: Management-Tool der Secure Digital Platform

sicherheitsrelevanten Vorfall welche Aufgabe hat, etwa durch die Ernennung eines Beauftragten für Cybersicherheit. Wir fokussieren uns hingegen auf die Technik. Wir bieten Unternehmen eine digitale Security-Plattform, die aus den Komponenten Management-Tools, Security-Gateways und Endpunkt-Lösungen besteht. Für die Integration des Systems beim Endkunden kooperieren wir dann mit verschiedenen Partnern.

gwf: Wie können wir uns die Funktionsweise der Plattform vorstellen – ist sie eine Art Antivirenprogramm?

Vallazza: Sie ist wesentlich mehr. Die Plattform bietet ein ganzes Bündel von Features: Firewall, VPN, Verschlüsselung und ein lückenloses Monitoring aller Komponenten, sodass der Nutzer immer weiß, was wann wo passiert. Mit diesen Elementen lässt sich eine sogenannte Zero-Trust-Architektur umsetzen, in der jeder Netzwerk-Teilnehmer über mehrere Faktoren authentifiziert wird. Hinzukommt eine Autorisierung nach dem Least Privilege-Prinzip: Es besagt, dass Benutzern, Systemen oder Anwendungen nur die Berechtigungen gewährt werden, die sie für die Erfüllung ihrer Aufgaben unbedingt brauchen.

gwf: Liefern Sie damit das technische Werkzeug, mit dem Betriebe die neuen Richtlinien umsetzen können?

Vallazza: Genau. Unsere Plattform bietet Unternehmen alles, um sich NIS-2-konform aufzustellen. Sie ist dabei so flexibel ausgelegt, dass sie in sämtlichen Branchen zum Einsatz kommen kann – gerade auch bei Betreibern von kritischen Infrastrukturen wie Gasnetzen und -speichern. Diese können mit der Plattform nicht nur die Sicherheit ihrer Anlagen erhöhen, sondern auch die Leistung sämtlicher Netzkomponenten monitoren. Dadurch lassen sich mögliche Schwachstellen im Netz aufdecken und Daten über den Energieverbrauch und die -effizienz sammeln.

gwf: Die Sofware, die das System aus Sicherheitsgründen überwacht, dient zugleich auch zur Überwachung der Performance?

Vallazza: Genau. Um ein System abzusichern, müssen Sie es segmentieren. Es ist wie auf einem Schiff: Tritt dort Wasser in ein Segment ein, kann ich es abriegeln und die Gefahr so lokal begrenzen. Das gleiche Konzept gibt es in der Cybersicherheit. Ich kann eine Anlage in möglichst viele, möglichst kleine digitale Einzelsegmente unterteilen, sogenannte Zones oder Conduits, die miteinander kommunizieren. Im Idealfall erfolgt diese Kommunikation nur von innen nach außen. Wenn ein Segment mit Schadsoftware infiziert ist, kann der Schaden so nicht auf die umliegenden Segmente übertragen werden und hat damit möglichst geringe Auswirkungen.

gwf: Ist diese digitale Segmentierung von Anlagen denn noch nicht Usus?

Vallazza: Nein, heute bilden Anlagen meist ein großes digitales Segment. Daher kann eine Arbeitsstation, die von einem Virus befallen ist, alle anderen Systemkomponenten infizie-

ren. Mit unserem Ansatz lässt sich ein infiziertes Segment einfach abschalten, isolieren und gesondert reparieren. Wir leisten also nicht nur Netzwerküberwachung, sondern auch die Überwachung jedes einzelnen Netzwerksegments.

gwf: Gerade Anlagensysteme im erneuerbaren Energiebereich bestehen oft aus vielen Elementen, etwa Elektrolyseure.
Vallazza: Korrekt. Cybersecurity wird beim Wasserstoff daher umso wichtiger sein. Die Infrastrukturen sind noch dezentraler als im klassischen Gassektor, und alles, was dezentral ist, ist schwieriger abzusichern. Jede Komponente ist ein mögliches Einfallstor für Cyberangriffe, und wenn diese nicht sauber voneinander abgeschottet sind, können von einem Punkt alle anderen infiziert werden. Für die Sicherheit und Effizienz solcher Anlagen wird eine vollständige Transparenz daher extrem wichtig sein. Nach heutigem Stand gibt es hier bei noch großes Verbesserungspotenzial.

gwf: Damit sprechen Sie einen Punkt an, der uns schon oft begegnet ist: Die Energiewende kommt ohne Digitalisierung nicht aus. Man könnte auch sagen: Erst die Digitalisierung, dann der Wasserstoff.
Vallazza: Ich würde sagen: Ohne Digitalisierung kein Wasserstoff – und ohne Cybersecurity keine Digitalisierung. Ohne digitale Transformation kann bald überhaupt kein Produktionsprozess mehr sicher betrieben werden. Daher richtet sich unsere Security Digital Platform an alle Branchen, die etwas produzieren, ob nun physische Waren oder Energie. Auf der digitalen Ebene ist gewissermaßen alles gleich; es geht immer um Daten, Zahlen, Bits und Bytes.

gwf: Welche Anforderungen stellt Ihre Software eigentlich an die Hardware?
Vallazza: Sie hat keine nennenswerten Hardwareanforderungen und kann auf jeder Hardware mit X86 Architektur und unterstützten ARM-Systemen laufen. Da es sich um dezentrale Installationen handelt, sind viele einzelne Gateways im Feldeinsatz. Auf diese verteilen wir die Rechenleistung, sodass sie die Daten lokal verarbeiten und filtern können, um das zentrale System im Rechenzentrum oder der Cloud zu entlasten. Es ist wie in der Natur: Pflanzen und Tiere beziehen ihre Energie auch nicht aus einer zentralen Quelle.

gwf: Aber die einzelnen Gateways werden wiederum zentral gesteuert.
Vallazza: Ja. Die Komplexität besteht darin, dass sich alle Gateways regelmäßig bei einer Zentrale melden müssen. Deshalb bildet unsere Architektur eine Mischung aus Security-Gateways und Management-Tools wie dem Switchboard, der zentralen Stelle, über die der Nutzer alles managen kann. Damit erhält er das Beste aus beiden Welten: Er verwaltet viele dezentrale Einheiten, aber so, als wäre es eine einzige Plattform.

gwf: Ihr Unternehmen hat sich in den letzten Jahren stark weiterentwickelt. Wohin soll die Reise gehen?
Vallazza: Mit der Security Digital Plattform haben wir unsere Vision gefunden. An ihr werden wir in den nächsten Jahren kontinuierlich weiterarbeiten, um ihr gewaltiges Potenzial zu heben. Unser Ziel ist, die Unternehmen auf die riesigen Herausforderungen vorzubereiten, die auf sie zukommen. Damit haben wir genug zu tun, denn die Schurken schlafen nicht. In der Cybersecurity müssen wir konstant up to date sein.

„Digitalisierung bedeutet Vernetzung, und Vernetzung bedeutet Unsicherheit“

gwf: Wird die digitale Welt immer gefährlicher?
Vallazza: Möglicherweise. Fakt ist: Alles wird digitaler. Digitalisierung bedeutet Vernetzung, und Vernetzung bedeutet Unsicherheit. Wir als Hersteller von Security-Software sehen unsere Funktion darin, Unternehmen bei der Bewältigung dieser Unsicherheit zu unterstützen. Aktuell sind wir in einer Phase, in der wir primär ein Bewusstsein für die Gefahren schaffen. Unsere Kunden sind geniale Unternehmen, teilweise Weltmarktführer in ihren Branchen, und wollen sich auf ihr Business fokussieren. Wir unterstützen sie in Sachen Cybersecurity.

gwf: Die „alten“ Industrien müssen sich also stärker mit dem Thema auseinandersetzen, während die „neuen“ Industrien wie die Wasserstoffbranche ein stärkeres Bewusstsein aufweisen.
Vallazza: Richtig. Cybersecurity muss immer ein fester Bestandteil der Architektur sein. Damit spiegelt die Energiewende ein paradoxes Phänomen wider, das wir auch in der digitalen Welt sehen: Alles wird vernetzter und zugleich dezentraler. Die Zukunft ist dezentral.

gwf: Herr Vallazza, vielen Dank für das Interview!

Weitere Informationen unter:
https://www.endian.com/de/