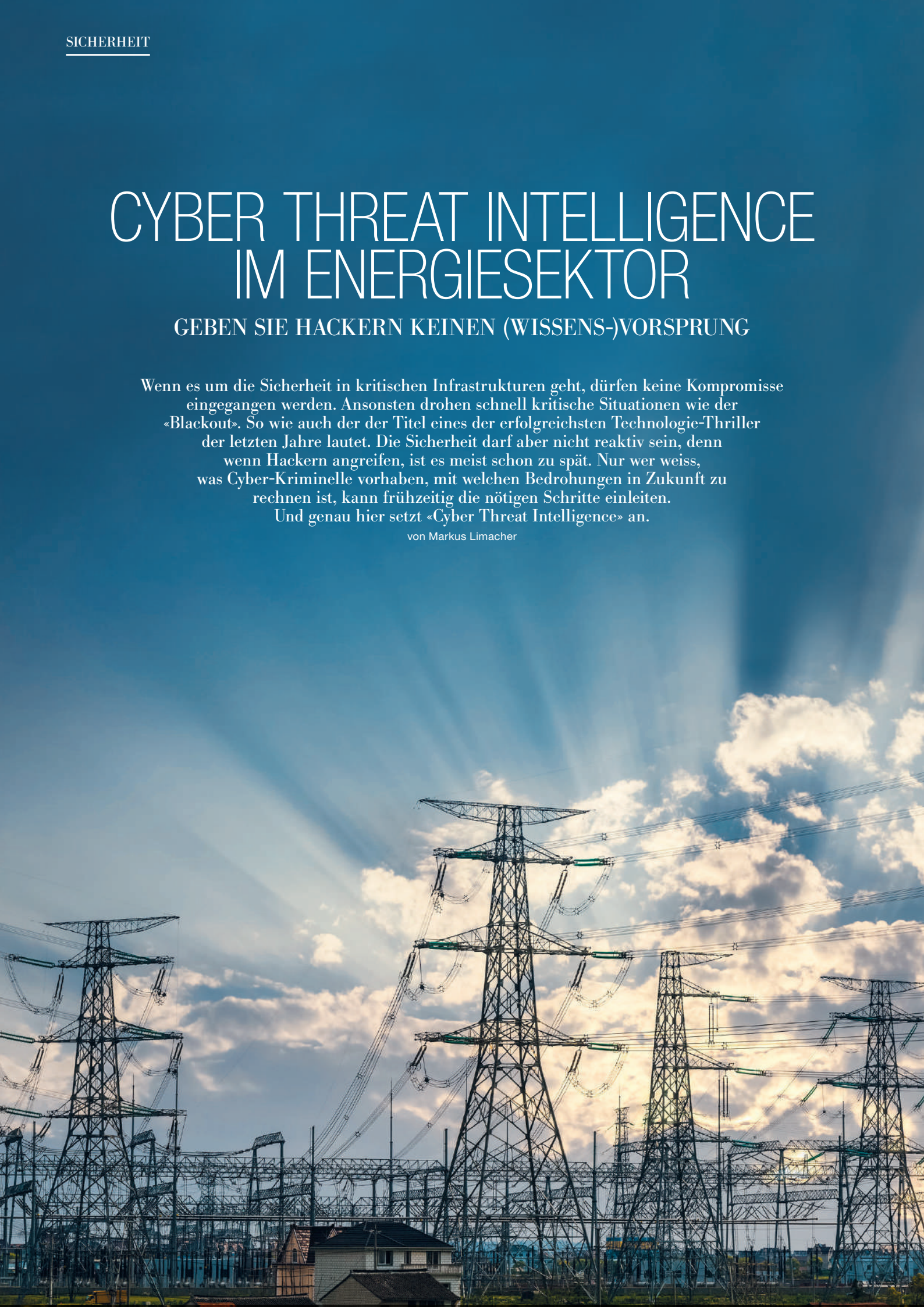
CYBER THREAT INTELLIGENCE IM ENERGIESEKTOR

GEBEN SIE HACKERN KEINEN (WISSENS-)VORSPRUNG

Wenn es um die Sicherheit in kritischen Infrastrukturen geht, dürfen keine Kompromisse eingegangen werden. Ansonsten drohen schnell kritische Situationen wie der «Blackout». So wie auch der der Titel eines der erfolgreichsten Technologie-Thriller der letzten Jahre lautet. Die Sicherheit darf aber nicht reaktiv sein, denn wenn Hackern angreifen, ist es meist schon zu spät. Nur wer weiss, was Cyber-Kriminelle vorhaben, mit welchen Bedrohungen in Zukunft zu rechnen ist, kann frühzeitig die nötigen Schritte einleiten. Und genau hier setzt «Cyber Threat Intelligence» an.

von Markus Limacher



Kritische Infrastrukturen, ob in den Bereichen Energie, Wasser oder Verkehr, sind auf funktionierende Systeme angewiesen. Die Absicherung von ICS- und SCADA-Systemen stellt Unternehmen jedoch vor eine Reihe von Herausforderungen. Bislang bewegten sich solche Steuerungs-Systeme in einer eigenen Welt proprietärer Protokolle, auf speziellen Plattformen und einer darauf zugeschnittenen Kommunikationsinfrastruktur. Sie waren von anderen Netzwerken – einschliesslich dem Internet – meistens isoliert. Durch die zunehmende Prozessintegration und Interoperabilität mit Partnern etc. wird immer häufiger auch Standard-Hard- und Software eingesetzt, welche über öffentliche Netzwerke angebunden werden. Dadurch sind diese Systeme und die mit diesen Systemen verbundenen Komponenten den bekannten Risiken und Bedrohungen ausgesetzt und angreifbarer. Erschwerend kommt hinzu, dass kritische Infrastrukturen ein attraktives Ziel für Hacker sind und die Zahl der Cyber-Angriffe seit Jahren exponentiell wächst, wie BlackEnergy, Dragonfly oder auch Sandworm drastisch belegen.

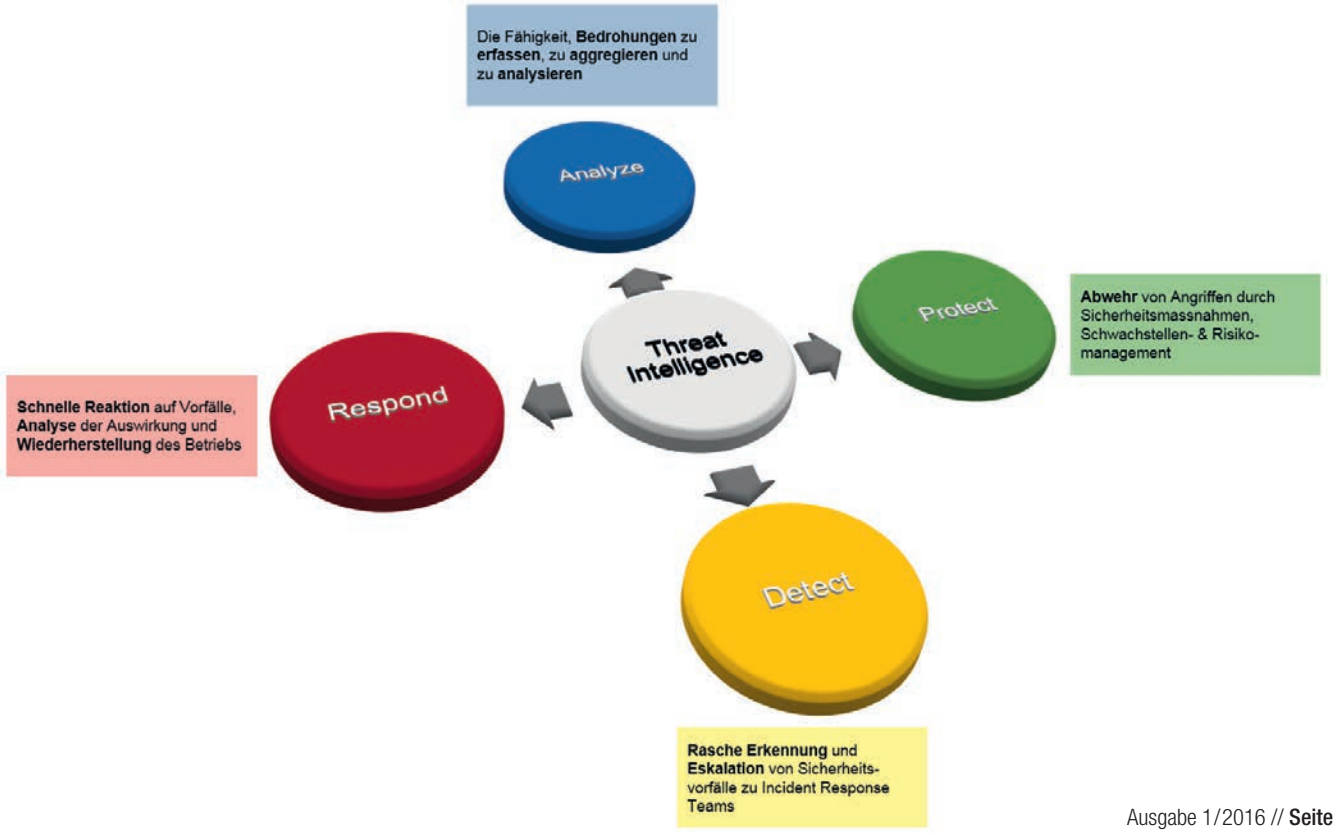
Traditionelle Netzwerkschutz-Tools wie Intrusion-Detection-Systeme und Anti-Virus-Lösungen haben den Fokus auf der Erkennung von Angriffen, wenn bereits erste Barrieren überwunden und ein Incident-Response-Verfahren gestartet werden soll. Eine kontinuierliche Professionalisierung der Angreifer und Weiterentwicklung von Einbrüchen und Verschleierungstaktiken definiert diese Sicherheitsansätze alleine als nicht ausreichend. Sicherheitsverantwortliche benötigen deshalb zur Überwachung und Optimierung der bestehenden präventiven Abwehr-Mechanismen aktuelle, detaillierte und zuverlässige Informationen über die sich ständig wandelnden und weiterentwickelnden Angriffsmethoden, wie beispielsweise Zero-Day Threats, Advanced Persistent Threats (APTs), DDoS Attacken, Ransomware und andere Bedrohungs-Szenaren. Aber genau diese Informationen findet man in den seltensten Fällen im öffentlichen Internet.

MIT WISSEN GEGEN DIE KRIMINELLEN

Es reicht nicht mehr sich reaktiv vor aktuellen Cyber Attacken zu schützen, heutzutage braucht es eine umfassende und präventive Threat Intelligence. Denn nur wer seine Gegner im Detail kennt, kann aus einer fundierten Informationsposition heraus agieren (und muss nicht kurzfristig oder überhastet reagieren). Nur so ist es möglich, auf Augenhöhe mit möglichen Angreifern zu bleiben und sich zuverlässig zu schützen. Gleichzeitig wird die Erfolgswahrscheinlichkeit für aktuelle und künftige Bedrohungen massiv einschränkt. Zudem treibt dies die Kosten und den Aufwand für die Angreifer in die Höhe.

Threat Intelligence ermöglicht es also Unternehmen, insbesondere auch aus dem Energiesektor, mit den immer anspruchs-

volleren und international organisierten Bedrohungen umzugehen. Dabei werden systematisch Daten über aufkeimende Bedrohungen und Trends gesammelt. Hierbei bedient man sich unterschiedlichster Quellen, wie dem Darknet, aber auch Tor Netzwerke, Hacker Foren, Internet, Blogs, Social Media, IRC Channels, etc. Diese Daten werden gefiltert, analysiert und korreliert, um daraus nützliche Informationen abzuleiten. Der erhebliche Mehrwert besteht darin, dank der frühen Kenntnis über neue Schwachstellen und dem Wissen über eine mögliche Ausnutzung dieser Schwachstellen aus erster Hand und direkt von der Quelle zu bekommen. Threat Intelligence unterstützt die Sicherheitsverantwortlichen proaktiv bei der frühzeitigen Identifizierung neuer Bedrohungen sowie bei der rechtzeitigen Einleitung geeigneter Massnahmen (aus dem ganzen verfügbaren Spektrum möglicher Massnahmen; ggf. intern, extern und mit Partnern und Providern zusammen) um einen erfolgreichen Angriff zu verhindern. ▸



360° SICHT AUF DIE INDIVIDUELLE BEDROHUNGSLAGE

Stand bis vor kurzem der reine Schutz vor Cyber Attacken im Zentrum der Sicherheitsbetrachtung, braucht es heute ein umfassendes Cyber Threat Management. Dieses zielt darauf ab, Bedrohungen zu erkennen, daraus die entsprechenden Lehren zu ziehen und somit mit den Angreifern stets Schritt zu halten. Wenn also Unternehmen über die relevanten (teilweise gar personalisierten) Threats so zeitnahe wie möglich im Bilde sind, dann können sie auch rechtzeitig mitigierende Massnahmen initiieren und das Schliessen von Sicherheitslücken einleiten, um das Risiko zu mindern oder gar zu verhindern.

Die Risikosituation und Bedrohungslage ändert sich stetig. Aus diesem Grund sind regelmässige Überprüfungen des Sicherheitsdispositivs nach neuen Bedrohungen und Schwachstellen unerlässlich. Deshalb sollten zur Kontrolle zusätzlich regelmässig Sicherheitsaudits, Penetration Tests und auch Vulnerability Scans durchgeführt werden. Nur so kann die Sicherheit an die aktuelle Risikosituation angepasst und optimiert werden. Führende Energiedienstleister haben den Mehrwert von Threat Intelligence aus professionellen internen und externen Quellen erkannt und nutzen diese Recherche, Analyse und Korrelation bereits zu ihrem Vorteil.

INFOGUARD AG SICHERT DIE ENERGIEVERSORGUNG

Der Schweizer Informationssicherheits-Experte InfoGuard bietet nebst einem individuellen Cyber Threat Intelligence Service eine umfassende Palette an geeigneten Massnahmen zum Schutz der Daten und Systeme im Energiesektor. Dazu zählen CISO as a Service, Sicherheitsaudits und Penetration Testing, aber auch Massnahmen zur Implementierung einer greifenden organisatorischen Sicherheit sowie technologische Sicherheitslösungen und Managed Services aus der Schweiz – angefangen von der Erstellung eines Zonenkonzeptes über den Perimeter Schutz bis hin zur Real Time Überwachung mittels eines Security Information and Event Management Systems (SIEM) aus dem ISO/IEC 27001 zertifizierten Cyber Defence Center in der Schweiz.

KONTAKT AUTOR

Markus Limacher
Senior Security Consultant
InfoGuard AG
Lindenstrasse 10
6340 Baar