PRESSECLIPPING

Kritische Infrastruktur effektiv schützen – Protect critical infrastructure effectively

Von Jakob Jung

MRZ 17, 2023 IBM, IS4IT

Kritische infrastrstuktur (KRITIS) ist besonders gefährdet. Wie Versorger optimal auf die aktuelle Bedrohungslage reagieren sollten, zeigt eine Zusammensarbeit von IBM und seinem Partner IS4IT.

Unternehmen und Organisationen der kritischen Infrastruktur (KRITIS) sind mehr denn je Gefahren durch Cyberkriminalität ausgesetzt. Hat ein Angriff Erfolg, kann das Auswirkungen auf die gesamte Gesellschaft haben. Managed Security Services, wie sie IS4IT und IBM anbieten, können die Unternehmen bei der frühzeitigen Erkennung und Abwehr unterstützen. Wer Durst hat, kann ihn in Deutschland ganz unkompliziert und kostengünstig mit einem Glas Leitungswasser stillen. Möglich machen das die strenge Trinkwasserverordnung, die die Qualitätsrichtlinien festlegt, und die über 9.000 Versorger, die das Wasser überprüfen und an die Haushalte verteilen.

Was, wenn der Versorger nicht sicher sein kann, ob das Wasser aus der Leitung den gewohnten Reinheitsgrad hat? Binnen kürzester Zeit wären mehrere Millionen Menschen vom Zugang zu sauberem Trinkwasser abgeschnitten. Die Auswirkungen auf den Alltag und die wirtschaftlichen Schäden wären enorm. Daher sind KRITIS ein beliebtes Ziel für Cyberkriminalität.

KRITIS – Pfeiler der modernen Gesellschaft

KRITIS – Das sind Unternehmen, Organisationen und Einrichtungen, deren Ausfall oder Beeinträchtigung erhebliche Folgen für das Gemeinwesen haben kann. Weitere Beispiele für KRITIS in Deutschland, neben Wasserversorgern, sind:

- Energieversorgung (Strom, Gas, Öl)
- Ernährungswirtschaft (Lebensmittelproduktion und -verteilung)
- Gesundheitswesen (Krankenhäuser, Apotheken)
- Informationstechnik und Telekommunikation
- Transport- und Verkehrswesen (Flughäfen, Bahnhöfe, Straßenverkehr)
- Finanz- und Versicherungswesen
- Medien und Kultur (Rundfunk und Fernsehen)
- Siedlungsabfallentsorung (nach BSIG)
- Staat und Verwaltung (Justizeinrichtungen, Regierung und Verwaltung, Parlament, Rettungswesen inkl. Katastrophenschutz)

Critical infrastrstucture (CRITIS) is particularly at risk. A collaboration between IBM and its partner IS4IT shows how utilities should best respond to the current threat environment.

Critical infrastructure companies and organizations (CRITIS) are more exposed than ever to cybercrime threats. If an attack is successful, it can have an impact on society as a whole. Managed security services, such as those offered by IS4IT and IBM, can help companies detect and defend against them early on. In Germany, anyone who is thirsty can quench it easily and inexpensively with a glass of tap water. This is made possible by the strict drinking water regulations that set the quality guidelines and the more than 9,000 utilities that test the water and distribute it to households.

What if the supplier can't be sure that the water coming out of the tap is of the purity level to which people are accustomed? Within a very short time, several million people would be cut off from access to clean drinking water. The impact on everyday life and the economic damage would be enormous. This is why CRITIS are a popular target for cybercrime.

CRITIS – pillars of modern society

CRITIS – These are companies, organizations and facilities whose failure or impairment can have significant consequences for the community. Other examples of CRITIS in Germany, besides water utilities, are:

- Energy supply (electricity, gas, oil)
- Food industry (food production and distribution)
- Healthcare (hospitals, pharmacies)
- Information technology and telecommunications
- Transportation and traffic (airports, train stations, road traffic)
- Finance and insurance
- Media and culture (radio and television)
- Municipal waste management (according to BSIG)
- State and administration (judicial institutions, government and administration, parliament, emergency services incl. disaster control)

Vollständigen Artikel finden Sie hier
https://security-storage-und-channel-germany.de/kritische-infrastruktur-effektiv-schuetzen-protect-critical-infrastructure-effectively/

Mit der Ausweitung des Kreises der sogenannten „Unternehmen im besonderen öffentlichen Interesse“ wurde im Rahmen des IT-Sicherheitsgesetzes 2.0 eine Kategorie geschaffen, mit der nun auch Unternehmen wie z.B. Hersteller/Entwickler/Zulieferer von Gütern oder wesentlicher Komponenten von Produkten betroffen sind, die mit kritischen Infrastrukturen zu tun haben.

Neue Vorgaben sorgen für mehr Schutz – fordern die Unternehmen aber auch heraus

Damit werden eine Vielzahl von Unternehmen und deren Lieferketten in Kürze vor neue Hürden gestellt, da die Anforderungen des Gesetzes bis zum 5. Mai 2023 umgesetzt sein müssen. Das IT-Sicherheitsgesetz 2.0 erweitert die deutsche KRITIS-Regulierung von 2015 deutlich – mit mehr Pflichten für einen größeren Betreiberkreis, höheren Cybersecurity-Anforderungen und mehr Befugnissen für den Staat und Regulierungsbehörden. Unter anderem sind die Angriffserkennung und die Meldung von Störungen jetzt vorgeschrieben. Kommen KRITIS dem nicht nach, drohen ihnen empfindliche Sanktionen und Bußgelder. Damit steigt nicht nur die Anzahl der Unternehmen und Organisationen, die sich zu den KRITIS zählen müssen, sondern auch die Pflichten, die sie binnen kurzer Zeit umsetzen sollen.

Manuel Noe, Geschäftsführer bei IS4IT Kritis GmbH: „Unternehmen, die schon viel im Web präsent sind wie Onlinehändler, können das meist problemlos umsetzen. Aber klassische KRITIS – wie Versorger – müssen hier nachlegen und unter anderem SIEM-Lösungen einsetzen.“ Die Abkürzung SIEM steht für Security Information and Event Management. Es handelt sich um ein softwarebasiertes Technologiekonzept aus dem Bereich des Sicherheits-Managements, mit dem ein ganzheitlicher Blick auf die IT-Sicherheit möglich wird. SIEM stellt eine Kombination aus Security Information Management (SIM) und Security Event Management (SEM) dar. Durch das Sammeln, Korrelieren und Auswerten von Meldungen, Alarmen und Logfiles verschiedener Geräte, Netzkomponenten, Anwendungen und Security-Systeme in Echtzeit werden Angriffe, außergewöhnliche Muster oder gefährliche Trends sichtbar.

Geopolitik, COVID-19 und wirtschaftliche Lage verschärfen Bedrohungslage

Dass die verstärkten Bemühungen, die KRITIS zu schützen, positiv zu bewerten sind, steht außer Frage. Das bestätigt der Blick auf die allgemein ernste Bedrohungslage:

With the expansion of the circle of so-called „companies in the special public interest“, a category was created under the IT Security Act 2.0 that now also affects companies such as manufacturers/developers/suppliers of goods or essential components of products that are involved with critical infrastructures.

New requirements provide more protection – but also challenge companies

As a result, a large number of companies and their supply chains will soon face new hurdles, as the requirements of the law must be implemented by May 5, 2023. The IT Security Act 2.0 significantly expands the 2015 German CRITIS regulation – with more obligations for a wider range of operators, higher cybersecurity requirements and more powers for the state and regulators. Among other things, attack detection and incident reporting are now mandatory. If CRITIS fail to comply, they face severe sanctions and fines. This not only increases the number of companies and organizations that must count themselves among the KRITIS, but also the obligations they are expected to implement within a short period of time.

Manuel Noe, Managing Director at IS4IT Kritis GmbH: „Companies that already have a large presence on the web, such as online retailers, can usually implement this without any problems. But classic KRITIS – like utilities – have to step up their game here and implement SIEM solutions, among other things.“ The abbreviation SIEM stands for Security Information and Event Management. It is a software-based technology concept from the field of security management that enables a holistic view of IT security. SIEM is a combination of Security Information Management (SIM) and Security Event Management (SEM). By collecting, correlating and evaluating messages, alarms and log files from various devices, network components, applications and security systems in real time, attacks, unusual patterns or dangerous trends become visible.

Geopolitics, COVID-19 and economic situation exacerbate threat situation

There is no question that the increased efforts to protect the CRITIS are positive. This is confirmed by a look at the generally serious threat situation:

Vollständigen Artikel finden Sie hier
https://security-storage-und-channel-germany.de/kritische-infrastruktur-effektiv-schuetzen-protect-critical-infrastructure-effectively/

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) erkennt einen Zusammenhang zwischen dem Angriffskrieg Russlands in der Ukraine und vermehrten Angriffsversuchen auf KRITIS. Seit Ende April 2022 beobachtet das BSI wiederholt Distributed Denial of Service (DDoS)-Angriffe von Hacktivisten auf Ziele in Deutschland und international.

Die knappen Ressourcen sind laut Noe eine weitere große Herausforderung. So haben Unternehmen mit mehr als 10.000 Mitarbeitern häufig nicht mal 100 IT-Fachkräfte. Eine 24/7-Überwachung lässt sich mit dieser kleinen Mannschaft in der Regel nicht umsetzen. Schon gar nicht nach COVID-19, wo sich viele Systeme öffnen mussten und noch komplexer wurden. „Stellen sie sich vor, dass ein Betreiber von einem Kernkraftwerk binnen kürzester Zeit statt 50 inzwischen 600 mobile Arbeitsplätze verwaltet – bei einem so schnellen Wandel können nicht alle Sicherheitslücken von Anfang an zu 100% geschlossen sein, wenn es auch so sein sollte."

Neben der schwierigen geopolitischen Lage und den Nachwirkungen der Pandemie sieht er zudem die wachsende Cyberkriminalität als großes Risiko: „Wir erleben einen Anstieg der organisierten Cyberkriminalität, internationale Hackergruppen agieren zunehmend professioneller und bieten hohe finanzielle Anreize. Alleine in Deutschland haben 46% der Unternehmen in den letzten 12 Monaten eine Cyber-Attacke erlebt. Diese Zahl wurde von der Statistica 2023 veröffentlicht."

Managed SOC: IT-Sicherheit in erfahrene Hände legen

Unternehmen, die die Anforderungen aus dem IT-Sicherheitsgesetz 2.0 bis Anfang Mai nicht aus eigener Kraft umsetzen können – auch weil sie vielleicht erst seit kurzem zum Kreis der KRITIS zählen – können die IT-Sicherheit über ein Managed-Service-Angebot schnell herstellen oder zumindest die richtigen Voraussetzungen schaffen. Sie erhalten dann – je nach Umfang der gebuchten Leistung – einen kompletten Rundumschutz. Auch die IS4IT hat solche Leistungen im Angebot. Ob und in welcher Form ein Managed SOC (Security Operations Center) für ein Unternehmen in Frage kommt, hängt von vielen Faktoren ab. Zunächst betrachten die Fachleute von IS4IT den Reifegrad des Kunden. Mitunter müssen die Systeme zunächst grundlegend optimiert werden und dann schrittweise um neue Elemente ergänzt werden. Das langfristige Ziel – auch vor dem Hintergrund der neuen gesetzlichen Anforderungen – ist ein leistungsfähiges SIEM.

The German Federal Office for Information Security (BSI) recognizes a connection between Russia's war of aggression in Ukraine and increased attack attempts on KRITIS. Since late April 2022, the BSI has observed repeated distributed denial of service (DDoS) attacks by hacktivists against targets in Germany and internationally.

Scarce resources are another major challenge, according to Noe. For example, companies with more than 10,000 employees often don't even have 100 IT professionals. 24/7 monitoring usually cannot be implemented with this small team. Especially not after COVID-19, where many systems had to open up and became even more complex.

„Imagine an operator of a nuclear power plant managing 600 mobile workstations within a very short time instead of 50 – with such rapid change, not all security gaps can be 100% closed from the start, even if they should be."

In addition to the difficult geopolitical situation and the aftermath of the pandemic, he also sees growing cybercrime as a major risk: „We are seeing a rise in organized cybercrime, international hacker groups are acting in an increasingly professional manner and offer high financial incentives. In Germany alone, 46% of companies have experienced a cyber attack in the last 12 months. This figure was published by Statistica 2023."

Managed SOC: Put IT security in experienced hands.

Companies that cannot implement the requirements of the IT Security Act 2.0 on their own by the beginning of May – also because they may have only recently become part of the KRITIS circle – can quickly establish IT security via a managed service offering or at least create the right conditions. They then receive – depending on the scope of the service booked – complete all-round protection. IS4IT also offers such services. Whether and in what form a Managed SOC (Security Operations Center) comes into question for a company depends on many factors. First of all, the experts at IS4IT look at the customer's maturity level. Sometimes the systems must first be fundamentally optimized and then gradually supplemented with new elements. The long-term goal – also against the background of the new legal requirements – is a powerful SIEM.

Vollständigen Artikel finden Sie hier
https://security-storage-und-channel-germany.de/kritische-infrastruktur-effektiv-schuetzen-protect-critical-infrastructure-effectively/

Noe beschreibt die Funktionen so: „Zunächst definieren wir, welche Instanzen wir schützen wollen. Dann binden wir diese an und das SIEM nimmt seine Analysetätigkeit auf. Im Bereich User Behavior Analytics erkennt es nach einer gewissen Zeit das typische Verhalten des Users – z.B. IP-Adresse, aktive Zeitfenster usw. Meldet sich ein User plötzlich aus einer völlig anderen Region, in einem anderen Netzwerkbereich oder mitten in der Nacht an, schlägt das SIEM Alarm. Hier gilt es auch die richtigen Schwellenwerte zu definieren. Nutzt das Unternehmen unseren 24/7-Service, prüft dann einer unserer 30 Analysten den Vorfall. So lassen sich Bedrohungen schnell identifizieren und abwehren."

Ein Managed-Service-Angebot wie es die IS4IT hat, ist grundsätzlich unabhängig von Herstellern und deren Tools. Im Bereich SIEM setzt IS4IT auf QRadar von IBM: „Wir schätzen die lange Erfahrung – über 30 Jahre – die IBM im Security-Umfeld mitbringt und die Zusammenarbeit auf Augenhöhe." Ein weiterer Vorteil ist die offene Architektur. So existieren bereits über 1.500 Anleitungen für Implementierungen im sogenannten Device Support Module Guide (DSM) und das Tool arbeitet problemlos mit anderen Security-Assets wie Splunk SIEM oder Google Chronicle zusammen. „Die heutige Bedrohungslandschaft fordert Sichtbarkeit, Automatisierung und kontextuelle Erkenntnisse mit einem robusten, offenen Ansatz. Da die IBM Security-Lösungen konsequent einem offenen Plattformgedanken folgen, lassen sie sich sogar binnen Stunden aufsetzen. Und je schneller ein Unternehmen wie ein Versorger reagieren kann, desto besser ist das für das Gemeinwohl", so Noe.

Noe erinnert sich: „Im Fall des Wasserversorgers wurden wir mit der Analyse eines zurückliegenden Angriffs beauftragt. Der Angriff erfolgte zeitgleich mit Beginn der Russland-Offensive im Februar 2022. Da das SIEM auch Altdaten analysieren kann, konnten wir die Quelle des Angriffs – in dem Fall war ein Lieferant betroffen – schnell ausfindig machen. Binnen fünf Stunden war das SIEM einsatzbereit. In so einem Fall setzen wir auch auf die „Indicator of Compromise"-Listen (IOC) des BSI und detektieren über über das SIEM z.B. bestimmte IP-Adressen, die laut IOC-Liste auf Kompromittierung hinweisen. Bei dem Wasserversorger konnten wir die Wirksamkeit des SIEM Systems deutlich am Verhalten der Firewall ablesen." Die Wasserversorgung von rund 4 Millionen Menschen war nie ernsthaft bedroht – und dank der Möglichkeiten des SIEM's und den erfahren IT-Fachkräften von IS4IT ist sie auch vor künftigen Angriffen sehr gut geschützt.

Noe describes the functions as follows: „First, we define which instances we want to protect. Then we bind them and the SIEM starts its analysis activities. In the User Behavior Analytics area, it recognizes the typical behavior of the user after a certain amount of time – e.g., IP address, active time windows, etc. If a user suddenly logs on from a completely different region, in a different network area or in the middle of the night, the SIEM raises an alarm. Here it is also important to define the right thresholds. If the company uses our 24/7 service, one of our 30 analysts then checks the incident. This allows threats to be quickly identified and defended against."

A managed service offering like IS4IT's is fundamentally independent of manufacturers and their tools. In the area of SIEM, IS4IT relies on QRadar from IBM: „We appreciate the long experience – over 30 years – that IBM brings to the security environment and the cooperation on an equal footing." Another advantage is the open architecture. For example, more than 1,500 implementation guides already exist in what's called the Device Support Module Guide (DSM), and the tool works easily with other security assets such as Splunk SIEM or Google Chronicle. „Today's threat landscape demands visibility, automation and contextual insights with a robust, open approach. Because IBM Security solutions consistently follow an open platform mindset, they can even be deployed within hours. And the faster a company can respond, like a utility, the better it is for the common good," Noe said.

Clean water, rather than systems hacked

Noe recalls, „In the water utility's case, we were tasked with analyzing a past attack. The attack coincided with the start of the Russia offensive in February 2022. Because the SIEM can analyze legacy data, we were able to quickly pinpoint the source of the attack – in that case, a supplier was affected. Within five hours, the SIEM was up and running. In such cases, we also rely on the BSI's Indicator of Compromise (IOC) lists and use the SIEM to detect, for example, certain IP addresses that indicate compromise according to the IOC list. At the water utility, we could clearly see the effectiveness of the SIEM system in the behavior of the firewall." The water supply of about 4 million people was never seriously threatened – and thanks to the SIEM's capabilities and IS4IT's experienced IT professionals, it is also very well protected against future attacks.

Vollständigen Artikel finden Sie hier
https://security-storage-und-channel-germany.de/kritische-infrastruktur-effektiv-schuetzen-protect-critical-infrastructure-effectively/