Sommer 2024

SEC COM

Security Magazin

Sicherheitstechnik für Ihr Business

Mehr Flexibilität für Klaas Kranbau

Seite 4
NIS-2
Herausforderung für die Unternehmenssicherheit

Seite 10
Alarmserver
Ganz automatisch alles im Blick behalten

Seite 14
SEC-COM 2024
Alle Informationen zu unserer Messe

Inhalt

04 NIS-2
Neue EU-Richtlinie fordert strengere Vorkehrungen bei der IT-Sicherheit

06 Hackerangriffe
Was man wissen muss um sein Unternehmen effektiv zu schützen

07 Firewall
Das wichtigste Werkzeug gegen Cyberkriminelle kurz vorgestellt

08 Kundenreferenz
Türen bei Klaas Alu-Kranbau für bessere Kommunikation geöffnet

10 Interview
„Ein Alarmserver kann auf ganz vielfältige Weise unterstützen“

12 Brandmeldetechnik
Warum man den Brandschutz für Unternehmen ernst nehmen muss

14 SEC-COM 2024
Alles was man für den Besuch unserer Messe wissen muss

Impressum:

Herausgeber:

SEC-COM Sicherheits- und Kommunikationstechnik GmbH
Am Stadion 117
45659 Recklinghausen
Tel.: 02361/9322-0
E-Mail: info@sec-com.de

Redaktion SEC-COM:
Folker Lück, tellyou redaktionsbüro

Layout & Umsetzung:
SEC-COM GmbH, Tanja Otterbein

Fotos SEC-COM:
Nils Vespermann

Reproduktion & Verfielfältigung:

Nur nach ausdrücklicher Genehmigung der SEC-COM GmbH

qualityaustria
SYSTEMZERTIFIZIERT
ISO 9001:2015 NR.21628/399

Gehören Sie zu den 40.000?

Liebe Leserinnen und Leser,

unser Kundenmagazin SEC-COM Security informiert in jeder Ausgabe zu den Chancen und Möglichkeiten, die sich durch Investitionen in moderne Sicherheitslösungen für Ihr Unternehmen oder Ihre Organisation ergeben können.

In dieser Ausgabe machen wir Sie allerdings auch auf ein neues Regelwerk der EU aufmerksam, bei dem es nicht um Optionen oder Kann-Empfehlungen geht. Vielmehr stehen in der neuen NIS-2-Richtlinie klare Anforderungen, die hinsichtlich Cybersicherheit künftig eingehalten werden müssen. Sie werden dafür keinen Brief von staatlicher Stelle erhalten, wie man das etwa vom Finanzamt her kennt. Vielmehr gilt es, sich aktiv zu informieren und die Regeln umzusetzen. Wer das versäumt, muss nicht nur mit teils drakonischen Strafen rechnen. Ebenso schmerzlich kann es sein, dass man Geschäftspartner verliert, die aufgrund ihrer Größe selbst die Richtlinien einhalten müssen und die künftig nur noch mit solchen Betrieben kooperieren dürfen, die selbst auf gleiche Weise geschützt sind. Ganz wichtig: Die neue NIS-2-Richtlinie betrifft rund 40.000 Unternehmen alleine in Deutschland! Dazu gehören folglich nicht nur große Konzerne, sondern auch sehr viele mittelständische Betriebe. In dieser Ausgabe der SEC-COM Security informieren wir Sie ausführlich über NIS-2 und über die technischen Möglichkeiten, wie Sie alle gesetzlichen Anforderungen erfüllen. Gerne steht Ihnen hier unser gesamtes Team mit Rat und Tat zur Seite!

Eine tolle Erfolgsgeschichte aus dem Münsterland ist der Bericht über das Unternehmen Klaas Service- und Vertriebs GmbH. Der leistungsstarke Maschinenbauer produziert aus dem leichten Werkstoff Aluminium beispielsweise Baukräne und Aufbauten für Feuerwehrfahrzeuge. Alles „Made in Germany“ und nach der weltweit anerkannten ISO 9001-Norm zertifiziert. Kein Wunder, das die Technik von Klaas international gefragt ist! Einen Neubau am Hauptstandort von Klaas in Ascheberg rüstete SEC-COM mit einem modernen, digitalen Schließsystem des Herstellers DOM aus. Die gute Zusammenarbeit mit unserem Unternehmen im Bereich der Sicherheitstechnik führte letztlich dazu, dass unsere Expertise auch für neue Lösungen in den Bereichen Kommunikation und IT nachgefragt wurde. So nutzt das Unternehmen jetzt eine moderne Mitel-Kommunikationsplattform, ein optimiertes WLAN und weitere Technologie, die von SEC-COM zuverlässig integriert wurde. Klaas konnte auf diese Weise die Erreichbarkeit des Serviceteams massiv verbessern.
Insgesamt ist der erfolgreiche Mittelständler jetzt im Geschäftsalltag noch flexibler unterwegs! Wir wünschen weiterhin viel Erfolg!

Im Interview mit unserem Alarmserver-Fachmann Tim Parthum versteht man schnell, dass diese Technologie keineswegs etwas „Exotisches“ für ein paar Sonderfälle ist. Vielmehr wird deutlich, dass Alarmserver für eine Vielzahl von Anwendungsszenarien genau das Richtige sind. Dabei geht es etwa um ein Höchstmaß an Patientensicherheit in Krankenhäusern, aber auch um die sichere Evakuierung bei einem Ereignis in nahezu jedem Bürogebäude. Alarmserver können noch viel mehr, zum Beispiel für eine reibungslose Produktion im Lebensmittelsektor sorgen oder davor warnen, wenn sich unbefugte Personen auf dem Betriebsgelände aufhalten. Am besten lesen Sie selbst!

Brandmeldeanlagen sind wichtig, denn sie können Menschenleben retten. Wir stellen Ihnen vor, was die heute aktuellen Lösungen leisten und erläutern, warum vernünftiger Brandschutz nicht etwa zu den lästigen Bauvorschriften zählt, sondern unbedingt eingehalten werden muss. Wir von SEC-COM unterstützen Sie dabei und sorgen auch dafür, dass die vorhandene Technik für viele Jahre zuverlässig funktioniert.

Ich wünsche Ihnen einmal mehr aufschlussreiche Leseminuten mit der SEC-COM Security.

Herzlichst, Ihr

Guido Otterbein
Geschäftsführer und Inhaber

NIS-2: Hoher Aufwand für mehr Sicherheit

Jedes Unternehmen sollte Maßnahmen ergreifen, um sich vor Angriffen von Cyberkriminellen zu schützen. Für immer mehr Unternehmen ist das aufgrund der neuen NIS-2-Richtlinie nicht nur empfehlenswert, sondern gesetzlich verpflichtend. Auch viele mittelständische Betriebe sind betroffen.

Foto: istock - Vitalii Gulenok

Die Zahl der kriminellen Cyberangriffe in Deutschland liegt kontinuierlich auf hohem Niveau. Laut Bundeskriminalamt (BKA) wurden zuletzt exakt 136.865 entsprechende Fälle für den Zeitraum eines Jahres registriert. Allerdings schätzt das BKA selbst die Dunkelziffer auf beträchtliche 90 Prozent - das heißt, von zehn Fällen wurde nur einer tatsächlich angezeigt.

Die ab Oktober 2024 geltende EU-Richtlinie NIS-2 ist eine überarbeitete Version der NIS-1-Richtlinie, die strengere Cybersicherheitsstandards für viele Unternehmen vorschreibt. Die strengeren Vorschriften werden als Reaktion auf die erhöhte Bedrohung durch digitale Angreifer eingeführt. Ziel der Richtlinie ist es, potenziell katastrophale Angriffe auf wichtige Unternehmen zu verhindern. In Deutschland sind schätzungsweise bis zu 40.000 Unternehmen von den neuen NIS-2-Regelungen betroffen.

Im Zuge der NIS-2 hat sich die Zahl der betroffenen Branchen und Sektoren erweitert. Hierbei unterscheidet NIS-2 zwischen „wesentlichen" („Essential") und „wichtigen" („Important") Sektoren. Anhand von zwei Kriterien können Firmen schnell abschätzen, ob sie betroffen sind (siehe Kasten).

Für Unternehmen mit weniger als 50 Mitarbeitenden oder zehn Millionen Euro Jahresumsatz greift NIS-2 eigentlich nicht. Allerdings könnten von NIS-2 betroffene Organisationen gezwungen sein, in der gesamten Lieferkette strenge Sicherheitsvorkehrungen durchzusetzen. Das heißt: Sie könnten auch kleinste Lieferanten dazu verpflichten, Maßnahmen zu ergreifen – andernfalls könnten sie den Lieferantenstatus verlieren.

Wichtig: Wenn ein Unternehmen in mehreren Mitgliedsstaaten der EU tätig ist, muss es sich in jedem Mitgliedsstaat bei der zuständigen Behörde registrieren und die jeweiligen Vorschriften einhalten. In Deutschland müssen sich Unternehmen beim Bundesamt für Sicherheit in der Informationstechnik (BSI) registrieren.

Was Unternehmen tun müssen

Folgende Cybersecurity-Maßnahmen müssen betroffene Unternehmen umsetzen:

- Richtlinien für Risiken und Informationssicherheit erstellen und umsetzen
- Prävention, Detektion und Bewältigung von Cybersecurity-Vorfällen (Sicherheitspannen)
- Betrieb eines Business Continuity Managements (BCM) inkl. Backup- bzw. Krisen-Management
- Gewährleistung der Sicherheit bei der Beschaffung von IT- und Netzwerk-Systemen
- Beachtung von Vorgaben für Kryptographie bzw. Verschlüsselung
- Umsetzung angemessener Maßnahmen zur Zugangskontrolle
- Einsatz sicherer Sprach-, Video- und Text-Kommunikation
- Einsatz gesicherter Notfall-Kommunikations-Systeme
- Überprüfung der Sicherheit in der gesamten Lieferkette
- Schulung und Sensibilisierung von Beschäftigten

Kurzum: Die „Hausaufgaben“, die auf von NIS-2 erfasste Einrichtungen zukommen, sind umfangreich und mit hohem Aufwand verbunden. Unternehmen sollten deshalb kurzfristig überprüfen, ob sie unter NIS-2 fallen. Betriebe sollten außerdem frühzeitig ausreichende Ressourcen in finanzieller, personeller und zeitlicher Hinsicht einplanen.

Angriffe unbedingt melden

Für die betroffenen Unternehmen gelten künftig Meldepflichten. Gemäß der NIS-2-Richtlinie müssen Vorfälle (erfolgte Cyberattacken) innerhalb von 24 Stunden nach Bekanntwerden gemeldet werden. Innerhalb von 72 Stunden nach der Meldung erfolgt gegebenenfalls eine Aktualisierung und erste Bewertung. Abschließende Berichte müssen spätestens einen Monat nach Bekanntwerden des Vorfalls dem BSI vorgelegt werden. Die neuen Meldepflichten sollen mehr Transparenz bringen und die koordinierte Bekämpfung von Cybersicherheitsvorfällen gewährleisten.

Keine Übergangsfristen

Anders als bei der seit 2018 geltenden DSGVO sind bei der NIS-2-Richtlinie keine Übergangsfristen vorgesehen. Ab 18. Oktober 2024 fallen damit faktisch alle betroffenen Unternehmen unter die neuen Anforderungen, müssen sich bei den Behörden registrieren und können entsprechend durch diese kontrolliert werden. Halten sich Unternehmen nicht an die Vorschriften, kann es teuer werden. Die NIS-2 sieht höhere Bußgelder als beim Vorgänger NIS-1 vor. Je nach Größe und Bedeutung des Unternehmens können Bußgelder bis zu 10 Millionen Euro oder zwei Prozent des weltweiten Jahresumsatzes (je nachdem, welcher Betrag höher ist) verhängt werden.

Verantwortliche haften persönlich

Um den Handlungsdruck zu erhöhen, will das Bundesinnenministerium laut einem Entwurf sogar die persönliche Haftung von verantwortlichen Managern durchsetzen. Demnach sollen die Leitungsorgane von Unternehmen für die Einhaltung der Risikomanagementmaßnahmen mit ihrem Privatvermögen haften. Die Obergrenze für diese Haftung entspricht zwei Prozent des globalen Jahresumsatzes des jeweiligen Unternehmens. Bei nachgewiesener Verletzung der Überwachungspflichten haftet ein Geschäftsleiter für die entstandenen Schäden. Selbst wenn hinterlegt ist, dass die Einrichtung auf Ersatzansprüche gegen den Chef verzichtet, haftet der Geschäftsführer persönlich, da eine solche Vereinbarung als unwirksam gewertet wird.

Fazit

Die EU verfolgt mit der neuen NIS-2-Richtlinie ein hehres Ziel: Sie will die EU-Staaten für Cyberangreifer zur Trutzburg machen. Durch hohe Sicherheitsvorkehrungen soll jede Attacke so aufwendig werden, dass sie sich kaum lohnt.
Für die Bürger – also uns alle – sind das prinzipiell gute Nachrichten. Niemand mag sich ausmalen, was passiert, wenn die IT ganzer Branchen lahmgelegt wird. Schon ein ausgefallener Energieerzeuger oder ein lahmgelegtes Krankenhaus führen zu großen Problemen. Doch die strengen Vorschriften setzen viele Unternehmen massiv unter Druck. Die Umsetzung der EU-Richtlinie kostet viel Geld, Zeit und personelle Ressourcen. Doch den Kopf in den Sand zu stecken, hilft nicht, denn die Bedrohung ist real! Wir alle müssen uns vor Cyberkriminellen besser verteidigen und diese Aufgaben ernst nehmen.

Von NIS-2 betroffene Unternehmen

1. Kriterium: Die Unternehmensgröße
- mindestens 50 Mitarbeitende
- Jahresumsatz/Jahresbilanz übersteigt 10 Millionen Euro

2. Kriterium: Der Unternehmenssektor
In der NIS-2 gibt es elf „wesentliche“ und sieben „wichtige“ Sektoren. Erfüllt ein Unternehmen die Kriterien der Unternehmensgröße und ist in den folgenden Sektoren tätig, so unterliegt es der NIS-2.

Wesentliche Sektoren	Wichtige Sektoren
1. Energieversorger	1. Post- und Kurierdienste
2. Transportwesen (z.B. Schienenverkehr, Busunternehmen, Spedition etc.)	2. Abfallwirtschaft
3. Bankwesen	3. Herstellung, Produktion und Vertrieb von Chemikalien
4. Finanzmarktinfrastruktur	4. Lebensmittelproduktion, -verarbeitung und -vertrieb
5. Gesundheit (einschl. Arzneimittel-Hersteller)	5. Hersteller von medizinischen Geräten, von Computern und Elektronik, von Maschinen und Ausrüstungen, von Kraftfahrzeugen, Anhängern und Sattelanhängern und sonstigen Transportgeräten
6. Trinkwasser	6. Digitale Anbieter (Online-Marktplätze, -Suchmaschinen und Social-Networking-Service-Plattformen)
7. Abwasserwirtschaft	7. Forschungseinrichtungen
8. Digitale Infrastruktur	
9. IKT-Dienstleistungsmanagement (B2B)	
10. Öffentliche Verwaltungen	
11. Weltraumwirtschaft	

Hackerangriff: Vorsorge ist besser!

Cyberangriffe sorgen inzwischen jede Woche für Schlagzeilen. Große Konzerne und öffentliche Einrichtungen werden ebenso angegriffen wie Organisationen im Gesundheitswesen und kleine und mittlere Unternehmen. Doch warum ist das eigentlich so?

Die Antwort auf die Frage, warum es immer mehr Hackerangriffe gibt, ist ziemlich banal: Weil es sich lohnt! Täglich gelingt es, irgendwo auf der Welt ganze Firmennetze lahmzulegen, sensible Daten zu stehlen oder Betriebe zu erpressen. Wichtig zu wissen: Auch die Anzahl von Angriffen auf Geheiß uns feindlich gesonnener Staaten hat zugenommen! Ganze Heerscharen von Hackern programmieren und verbreiten Malware, die über das Internet jedes vernetzte Gerät erreichen können. „Jedes vernetzte Gerät“ heißt: Nicht nur den PC auf dem Büro-Schreibtisch, sondern auch das Smartphone, den Drucker, das vernetzte Medizingerät des Hausarztes oder den supermodernen, vernetzten Kühlschrank!

Goldwährung Kundendaten

Doch nicht nur manche Staaten wollen Schaden anrichten und unsere Technik sabotieren. Auch hunderttausende private Cyber-Kriminelle beschäftigen sich Tag für Tag damit. Im Dark Net werden fertige Module angeboten, mit denen selbst Kleinkriminelle ganz ohne Programmierkenntnisse Schadsoftware gezielt einsetzen und verbreiten können. Die „Kunden“ solcher Technik agieren wie die Besucher in einem riesigen Spielcasino. Sie wissen, dass ihre Chancen nicht sonderlich hoch sind. Aber mit etwas Glück gibt es den „Hauptgewinn“: Dann erbeuten sie die Kundendaten eines Unternehmens oder die Patientendaten eines Krankenhauses. Solche Daten sind so wertvoll wie Bargeld: Man kann sie gewinnbringend veräußern oder das betroffene Unternehmen damit erpressen.

Mit SEC-COM das Sicherheitslevel erhöhen

Wir schützen Ihr Firmennetzwerk vor kriminellen Hackern, die es auf Ihre Kundendaten abgesehen haben oder ihr Netzwerk verschlüsseln, um dann ein Lösegeld zu erpressen. Wir sorgen dafür, dass ihr Netzwerk auch bei hoher Last nicht erlahmt und der Speicherplatz niemals zuneige geht.

Sie haben Fragen? Schreiben Sie uns jetzt gleich eine E-Mail oder rufen Sie uns an!

Ransomware-Erpressung

Das gleiche Ziel verfolgt die Verbreitung sogenannter Ransomware: Die Angreifer versuchen, in ihrem Netzwerk ein kleines Programm zu installieren, das sämtliche Daten in ihrem Firmennetzwerk verschlüsselt und damit unzugänglich macht. In manchen Fällen sind Hard- und Software so sehr beschädigt, dass nur noch die Neuanschaffung sämtlicher IT-Ausstattung möglich ist. Wer dann nicht vorgesorgt und alle wichtigen Unternehmens- sowie Kundendaten mittels Backups sorgsam gesichert hat, steht vor einem wahren Desaster!

Unzählige Phishing-Fallen

Auch das sogenannte „Phishing“ ist nach wie vor lukrativ für Cyber-Betrüger. Die Opfer einer Phishing-Attacke geben sensible Daten unwissend an Betrüger weiter, welche diese zu kriminellen Zwecken missbrauchen. Am häufigsten geschieht dies über Phishing-E-Mails und Phishing-Websites. Dabei handelt es sich um gefälschte Inhalte, die denen einer echten Organisation ähneln. Besonders beliebt sind gefälschte Webseiten oder E-Mails von Banken, Versicherungen, von Speditionsdiensten, Behörden und Software-Anbietern. Unter einem Vorwand einer Kontenblockierung, einem Gewinnspiel oder der Zahlung einer Gebühr werden die Opfer aufgefordert, sensible Daten anzugeben. Da die Inhalte der E-Mail oder der Webseite dem Original oft stark ähneln, wird die Fälschung meist nicht erkannt.

Wichtig zu wissen

Die „Kreativität“ der Kriminellen ist groß und die Zahl der Angreifer ist riesig. Deshalb ist es wichtig, die Widerstandsfähigkeit in ihrem Unternehmensnetzwerk zu erhöhen und hier kontinuierlich nachzubessern. Durch Prävention einen Angriff zu vermeiden ist ganz sicher das beste Rezept. Doch jeder Betrieb sollte zusätzlich einen „Plan B“ in der Schublade haben: Wenn ein Angriff gelingt, dann ist es am wichtigsten, dass alles so schnell wie möglich wieder funktioniert. Der denkbar schlechteste Weg ist es, auf Erpressungsversuche einzugehen! Damit unterstützt man Kriminelle und wird womöglich doppelt geschädigt. Denn niemand garantiert, dass die Diebe „ehrlich“ sind und nach einer Lösegeldzahlung alles wieder funktioniert.

Foto: istock - AndreyPopov

Die Brandmauer für Ihr IT-Netzwerk

Eine Firewall alleine sichert kein Computernetzwerk gänzlich ab. Ihre volle Wirkung entfacht die Technologie dann, wenn sie zum Bestandteil eines gesamten Sicherheitskonzepts wird.

Der englische Begriff Firewall steht für „Brandmauer“. Reale Brandmauern dienen dazu, das Übergreifen von Feuer und Rauch von einem Gebäude oder Gebäudeteil zu einem anderen zu verhindern. Ganz ähnlich muss man sich die Leistung von Firewalls in der Informationstechnologie vorstellen. Eine Firewall dient dazu, ungewollte Zugriffe auf ein Unternehmensnetzwerk zu unterbinden. Sie orientiert sich dabei an den Adressen der Kommunikationspartner und „weiß“, wer worauf zugreifen darf – und wer nicht. Eine Firewall blockiert selektiv Datenpakete oder lässt diese zu.

Grundsätzlich unterscheiden muss man zwischen einer Personal Firewall und einer externen Firewall (auch Netzwerk- oder Hardware-Firewall). Die „Personal Firewall“ ist eine Software, die auf ebenjenem Gerät installiert ist, dass sie schützen soll. Die Software einer externen Firewall arbeitet hingegen nicht auf dem zu schützenden System selbst, sondern auf einem separaten Gerät, das Netzwerke oder Netzsegmente miteinander verbindet und – wie bei der realen Brandmauer - gleichzeitig den Zugriff zwischen den Netzen beschränkt.

Firewall ist unverzichtbar

Doch wovor genau schützt eine Firewall eigentlich? Das kann beispielsweise schädliche Software sein, sogenannte Malware. Das sind Viren oder Spyware, die einen Rechner oder das gesamte Firmennetz befallen, um sensible Daten zu sammeln oder zu verändern. Schlimmstenfalls wird das Betriebssystem des Rechners oder das gesamte Firmennetz komplett lahmgelegt. Eine Firewall kann dazu beitragen, das zu verhindern.
Gerade dort, wo der Zugriff auf Internetinhalte unverzichtbar ist, leistet eine Firewall wertvolle Dienste. So kann beispielsweise die Filterung von gefährdeten ActiveX-Objekten aus Webseiten vorgenommen werden. Der Internetbrowser kann dann auf solche in einer Webseite eingebetteten Objekte nicht mehr zugreifen. Vorteilhaft daran ist, dass über diese Objekte kein Angriff erfolgen kann.
Dabei hilft die Erstellung eines Sicherheitskonzepts. In größeren Organisationen kommt dafür üblicherweise eine eigene Sicherheitsrichtlinie zum Einsatz.

Bestandteil an Gesamtkonzept

In einem modernen Firmennetzwerk sollte die Firewall ein Teilaspekt des Sicherheitskonzepts sein. So wie allein die Installation von Rauchmeldern noch kein wirkungsvoller Brandschutz ist, sollte auch der Einsatz einer Firewall je nach Sicherheitskonzept ein Element mehrerer Maßnahmen sein.
Im gemeinsamen Beratungsgespräch mit Ihnen finden wir genau das passende Security-Konzept, das Ihr Unternehmen bestmöglich schützt, ohne dass ihr Team im täglichen Workflow ausgebremst oder behindert wird. Sprechen Sie uns gerne jederzeit an, wenn Sie an einem unverbindlichen Gesprächstermin mit unseren Experten interessiert sind!

Bedrohung für kleine und mittelgroße Unternehmen

Laut einem im Frühjahr 2024 veröffentlichten Report des IT-Security-Spezialisten Sophos leiden kleine Unternehmen proportional stärker unter den Folgen von Cyberangriffen. Bei fast der Hälfte aller Angriffe auf kleine und mittlere Unternehmen (KMUs) kommen Keylogger, Spionagesoftware und sogenannte Stealers zum Einsatz. Das ist Schadsoftware zum Stehlen von Daten und Zugangsdaten. Cyberkriminelle nutzen diese Informationen später für unautorisierten Fernzugriff, Erpressung oder das Installieren von Ransomware.
Hier der vollständige Report „2024 Sophos Threat Report: Cybercrime on Main Street“ zum Nachlesen:

Die Türen für bessere Kommunikation weit geöffnet

Titel-story

Mit SEC-COM verbindet das marktführende Unternehmen Klaas Alu-Kranbau inzwischen eine langjährige, vertrauensvolle Zusammenarbeit. Die Integration eines digitalen Schließsystems war sprichwörtlich der Türöffner. Heute setzt das Klaas-Team auch bei der Kommunikation, der IT-Sicherheit und dem WLAN-Netz auf die Kooperation mit SEC-COM.

Die Wurzeln des münsterländischen Unternehmens Klaas Alu-Kranbau GmbH reichen bis in die 30er Jahre des vergangenen Jahrhunderts zurück. Einst als Bauunternehmen von Theodor Klaas gegründet, brachte der familiengeführte Betrieb kurz nach dem Zweiten Weltkrieg den ersten Schrägaufzug auf den Markt, der die Arbeit – nicht nur im Baugewerbe - erheblich vereinfachte.

Aus der Bauexpertise heraus und verbunden mit Kenntnissen über die Vorteile des leichten Werkstoffs Aluminium, konstruierte der Betrieb Anfang der neunziger Jahre den ersten Alukran, der schnell auch international den Durchbruch schaffte. Hinzu kam die Entwicklung innovativer Sondermaschinen beispielsweise im Bereich der Feuerwehrtechnik. Das stark expandierende Unternehmen verfügt über zehn bundesdeutsche Standorte, wodurch überall eine möglichst große Kundennähe gewährleistet ist. Das Herz schlägt dabei weiterhin am Stammsitz in Ascheberg, wo auch die Mehrzahl der aktuell rund 400 MitarbeiterInnen beschäftigt ist.

Klaas setzt bewusst auf „Made in Germany“ und agiert damit erfolgreich auf dem Markt: Die allermeisten Bauteile werden im Ascheberger Werk selbst gefertigt, nur wenige Materialien hinzugekauft. Um den hohen Qualitätsstandard dauerhaft zu halten, entschied sich der Betrieb für den Aufbau eines effektiven Qualitätsmanagementsystems, das nach der weltweit anerkannten ISO 9001-Norm zertifiziert wurde.

Nachdem Klaas Alu-Kranbau im Jahr 2018 in einem Ascheberger Gewerbegebiet ein großes Grundstück erwerben konnte, folgten mit dem Bau einer neuen Servicehalle und nachfolgend eines Kundencenters mit Büros und einem großem Ausstellungs- und Veranstaltungsraum zahlreiche, bauliche Veränderungen. Die Bereiche Vermietung, Vertrieb und die Klaas Academy bezogen 2022 neue Räumlichkeiten gegenüber der Ascheberger Servicewerkstatt.

Verbunden waren diese Neubauten mit dem Umstieg auf ein modernes, digitales Schließsystem, produziert vom Hersteller DOM und integriert von SEC-COM. „Wir erhielten damit sprichwörtlich im Handumdrehen ganz neue Möglichkeiten“, freut sich Leiter Service Deutschland Tobias Klaas. Mit der Lösung konnte erstmals klar und einfach geregelt werden, welche Mitarbeitenden welche Bereiche betreten dürfen. „Kommt es zu Änderungen, weil neue Mitarbeiter hinzukommen oder jemand das Unternehmen verlässt, so können wir innerhalb weniger Minuten Änderungen vermerken und Schlüssel entsprechend neu programmieren“, verdeutlicht Klaas die Vorteile.

Schritt für Schritt voran

Die gute Zusammenarbeit mit SEC-COM im Bereich der Sicherheitstechnik führte letztlich dazu, dass die Expertise des Dienstleisters auch in den Bereichen Kommunikation und IT-Lösungen nachgefragt wurde. „Wir verfügen zwar selbst über eine kleine,

wirklich starke IT-Abteilung. Aber das Team ist in der Regel mit Tagesaufgaben so beschäftigt, dass keine Zeit für eigene IT-Projekte bleibt. Hier kam deshalb einmal mehr SEC-COM ins Spiel“, erläutert Tobias Klaas. So sollte das Techniker-Team aus Recklinghausen dafür sorgen, die Flächendeckung und Qualität des WLAN an den verschiedenen Standorten am Stammsitz zu optimieren.

Mehr Transparenz durch neue Kommunikationsplattform

Als größte Einzelmaßnahme seitens SEC-COM folgte eine Optimierung der Kommunikationstechnik, die neben dem Hauptsitz auch sämtliche Niederlassungen betraf. Bedarf für eine neue Lösung bestand hier, da das alte System in die Jahre gekommen war und sich zuletzt technische Störungen wie Gesprächsabbrüche häuften. SEC-COM empfahl hier nach einer gemeinsamen Abstimmungsrunde den Einsatz der Kommunikationsplattform Mitel 470 als neues „Herzstück“ am Hauptstandort. Die Kernanforderungen an eine neue Lösung waren schnell zusammengetragen: Grundsätzlich sollte sich die Erreichbarkeit des Serviceteams an allen Standorten verbessern. Zudem wünschte man sich mehr Transparenz: Wie viele Service-Anrufe werden wo pro Tag bearbeitet? Welcher Mitarbeiter ist gerade „frei“, wer berät gerade einen Kunden? Das alte System bot hier keine Einblicke. Als Auswertungs- bzw. Anzeigetool implementierte und konfigurierte SEC-COM ein Dashboard, wodurch jetzt auf einem Blick wichtige Anrufstatistiken sichtbar sind.

Auch ein einheitliches Callrouting für die Standorte und Mitarbeiter in Deutschland stand auf der Wunschliste weit oben und konnte mit der neuen Plattform realisiert werden. Dadurch unterstützen sich nun die Standorte je nach Auslastung gegenseitig besser. Videomeetings und der schnelle Austausch unter den Kollegen mittels Chatnachrichten gehören nun ebenfalls zum Businessalltag. „Unser Team hat sich schnell mit den neuen Möglichkeiten vertraut gemacht und sich daran gewöhnt“ freut sich Serviceleiter Tobias Klaas. Die von SEC-COM integrierte Lösung optimierte auf Anhieb den täglichen Workflow. Die neue Technik verbesserte darüber hinaus die IT-Sicherheit aufgrund der Standortvernetzung mittels VPN.

„Die raketenschnelle Integration der neuen Kommunikationslösung innerhalb von vier Tagen fand ich wirklich beeindruckend“
Tobias Klaas

Bis das umfangreiche Projekt erfolgreich abgeschlossen werden konnte, war einige Vorarbeit notwendig: Nach gründlicher Feinabstimmung mit den Verantwortlichen bei Klaas sollte der konkrete Roll-out innerhalb weniger Tage an allen Standorten abgeschlossen sein. Diese zeitliche und logistische Herausforderung gelang. Innerhalb von nur vier Arbeitstagen war SEC-COM Projektleiter Frank Wollny an allen Standorten vor Ort und sorgte für die Einrichtung und den Betrieb der neuen Kommunikationsplattform.

Deutlich an Flexibilität gewonnen

Das Kernziel der besseren Erreichbarkeit des Serviceteams konnte vollumfänglich erreicht werden. Neben der ebenfalls massiv verbesserten Transparenz kann Klaas Kranbau mit Hilfe der neuen Technik von SEC-COM jetzt im Geschäftsalltag viel flexibler agieren. Das Team kann sich standortübergreifend besser abstimmen und gegenseitig unterstützen – gerade in Ferienzeiten oder bei plötzlichen Krankheitsfällen ist das wertvoll und die Kunden honorieren die optimierte Leistung. Das macht sich auch daran bemerkbar, dass die Anzahl der Anrufe – und damit das Kundeninteresse - kontinuierlich wachsen.
„Rückblickend haben wir hier eine sehr gute Investition getätigt, die unser Unternehmen spürbar vorwärtsbringt. Wir können zwischenzeitlich von einer langen, vertrauensvollen Zusammenarbeit mit SEC-COM sprechen.“

Interview mit Tim Parthum

„Ein Alarmserver kann auf ganz vielfältige Weise unterstützen“

Alarmserver können vor Gefahren warnen, aber auch für einen sicheren, automatisierten Produktionsablauf sorgen. Warum Alarmserver gerade für Betriebe, die von KRITIS und NIS-2 betroffen sind, wertvolle Unterstützung leisten, erklärt Tim Parthum, Experte bei SEC-COM für alle Fragen rund um das Thema.

Foto: istock - witsarut sakorn

Security: Jeder hat schon mal von einem Server gehört - aber was ist ein Alarmserver?

Die Funktion eines Alarmservers muss man sich im übertragenen Sinn so vorstellen wie den freundlichen Mitarbeiter vom Pförtnerbüro, der genau weiß, wer im Betrieb welche Funktion hat und ob die Person gerade anwesend ist. Er merkt außerdem sofort, wenn es brennt oder eine andere, kritische Situation besteht und holt dann sofort Hilfe. Und für alle, die lieber Technikersprache sprechen: Ein Alarmserver ist ein automatisiertes, vernetztes, überwachendes System, das bei einem Ereignisfall in Sekundenschnelle reagiert, agiert und informiert.

Security: Für welche Anwender ist der Einsatz eines Alarmservers interessant?

Im Prinzip für jedes Unternehmen, denn ein Alarmserver kann überall dort wertvolle Hilfe leisten, wo viele Menschen zusammenarbeiten – oder auch dort, wo nur eine Person oder gar kein Mensch eine Aufgabe verrichtet, beispielsweise in einem Hochregallager oder in einem Kühlraum. Er wird immer dann aktiv, wenn ein zuvor definiertes Notfallszenario detektiert wird.

Security: Wie kann ein Alarmserver die Abläufe in einem Unternehmen oder in einem Krankenhaus konkret verbessern?

Er kann beispielsweise auslösen, dass wegen eines Feuers mittels Lautsprecherdurchsage dazu aufgefordert wird, ein Gebäude sofort zu verlassen. Ein Alarmserver kann bei einem Brand auch auslösen, dass der Fahrstuhl nicht mehr benutzt werden kann. In einem Krankenhaus kann der Alarmserver sofort Personal informieren, wenn ein Patient in Not ist. Das geschieht in Kombination mit einem Lichtrufsystem optisch, es kann aber auch eine Nachricht auf ein Mobiltelefon gesendet werden. Es gibt außerdem noch ganz andere

Szenarien: Der Alarmserver kann in einem Produktionsbetrieb das Band anhalten und den Produktionsleiter informieren, weil ein wichtiges Element für die Produktion fehlt oder es einen Defekt gegeben hat. Er kann in Kombination mit entsprechenden Sensoren auch überwachen, dass in der Lebensmittelproduktion die Kühlkette eingehalten wird. Muss ein Gebäude evakuiert werden, kann der Alarmserver im Zusammenspiel mit einem Zugangskontrollsystem darüber informieren, wer sich aktuell vor Ort befindet und wo genau sich eine bestimmte Person gerade aufhält. Kurzum: Ein Alarmserver kann auf ganz vielfältige Weise unterstützen, helfen und warnen.

Security: Gibt es Bereiche, in denen der Betrieb eines Alarmservers unverzichtbar oder sogar gesetzlich vorgeschrieben ist?

Ja, die gibt es definitiv! Beispielsweise machen Normen für Qualitätsmanagementsysteme wie DIN oder ISO den Einsatz oft erforderlich. Hier ist der Einsatz von Alarmservern oft unumgänglich. Außerdem wird eine Vielzahl von Unternehmen künftig gemäß den neuen EU-Richtlinien NIS-2 sowie EU RCE dazu verpflichtet und dafür haftbar gemacht, Mindestanforderungen an Cybersicherheit und Resilienz einzuhalten.
Die Zahl der regulierten Unternehmen wird dadurch stark ansteigen. Aktuelle Schätzungen gehen von rund 40.000 Unternehmen in Deutschland aus. Dazu zählen sehr viele mittelständische Betriebe aus ganz unterschiedlichen Branchen, aber sogar Kleinbetriebe können betroffen sein. Der Beitrag über NIS-2 in dieser Security-Ausgabe gibt einen genauen Überblick darüber, welche Betriebe das betrifft. Übrigens werden die Unternehmen nicht von der EU dazu aufgefordert, hier Maßnahmen zu ergreifen. Vielmehr muss jedes Unternehmen selbst herausfinden, ob es unter die NIS-2-Regelung fällt und dann aktiv dafür sorgen, dass die neuen Vorschriften erfüllt werden. Aber, keine Sorge: Wir lassen hier keinen unserer Kunden im Regen stehen. Wir unterstützen bei allen Fragen und bei der Umsetzung gerne!

Security: Welche technischen Voraussetzungen sollten gegeben sein, damit ein Alarmserver erfolgreich implementiert werden kann?

Grundsätzlich sollte eine IT-Infrastruktur vorhanden sein. Das ist wie im Verkehr: Wenn weder Straßen noch Schienen vorhanden sind, dann wird es schwierig! Eine Grundvoraussetzung ist darüber hinaus die technische Planung. Es müssen Schnittstellen vorhanden sein oder geschaffen werden, um einen Alarmserver sinnvoll in die vorhandene IT-Umgebung zu integrieren. Wenn es in einem Unternehmen Zweifel darüber gibt, ob aktuell die notwendigen technischen Voraussetzungen für den Alarmserver-Betrieb erfüllt werden, dann empfehle ich, uns anzusprechen. Wir prüfen das und schaffen die entsprechenden Bedingungen.

Security: Was sollten Unternehmen tun, die sich über den Nutzen eines Alarmservers ein genaueres Bild machen möchten?

Zuerst einmal sollte intern besprochen werden, welche Lösung man haben möchte oder welche Lösung künftig womöglich vorgeschrieben ist. Wie schon gesagt kann ein Alarmserver ja in ganz unterschiedlichen Bereichen eingesetzt werden. Wer die Funktionalität dann einmal live erleben möchte, kann entweder zu uns ins Haus kommen und sich hier unsere Testumgebung vorführen lassen. Alternativ können wir auch zum Kunden ins Haus kommen und dort eine Testumgebung installieren. Wichtig zu wissen ist, dass ein Alarmserver vielfältig erweitert werden kann. Fast jede Sonderlösung ist technisch machbar. Bei schwierigen Anforderungen muss man allerdings auch die entstehenden Kosten bedenken. Ich empfehle, SEC-COM zu kontaktieren, weil wir aufgrund der großen Bandbreite an bereits umgesetzten Projekten in ganz unterschiedlichen Branchen über viele Erfahrungswerte verfügen. Wir beraten herstellerunabhängig und bemerken etwaige Stör- oder Fehlerquellen oder problematische Szenarien. Es ist ja immer hilfreich, wenn ein Außenstehender einen Blick auf die Pläne wirft.

„Ein Alarmserver kann überall dort wertvolle Hilfe leisten, wo viele Menschen Zusammenarbeiten“
Tim Parthum

Brandmeldetechnik rettet Leben

Wer sein Auto in einer Feuerwehreinfahrt parkt, muss nicht nur mit einem „Knöllchen“ rechnen – ein dort geparktes Auto wird in der Regel abgeschleppt und man wäre unter dem Strich gleich mehrere hundert Euro los. Eine übertriebene Strafe? Ganz sicher nicht, denn wenn bei einem Wohnungs- oder Häuserbrand die Feuerwehr von einem parkenden Auto behindert wird, dann kann die dadurch verloren gehende Zeit Menschenleben kosten!

Dass sich Brandschutz bezahlt macht, untermauern zudem aktuelle Zahlen: So konnte nach Angaben des Statistischen Bundesamtes die Anzahl der Brandopfer in Deutschland seit dem Jahr 2001 um rund ein Drittel reduziert werden. Dennoch kamen alleine im Jahr 2022 bundesweit exakt 333 Menschen durch Rauch, Feuer und Flammen um.

Um das Risiko gefährlicher Feuerunfälle weiter zu verringern, ist der Einsatz von moderner Brandschutztechnik sinnvoll und unerlässlich. Die Kerntechnologie für den Brandschutz in Gebäuden heißt Brandmeldeanlage, kurz BMA. Die Vorteile einer Brandmeldeanlage liegen auf der Hand: Ihre Sensoren erkennen frühzeitig Rauch, Flammen, Hitze oder Gase. Die Technik sorgt zuverlässig für eine Alarmierung.

Sozusagen das Herzstück einer Brandmeldeanlage ist die Brandmeldezentrale (BMZ). Bei ihr werden alle eintreffenden Signale gebündelt und weiterverteilt. Die BMZ besteht in den meisten Fällen aus einer Steuereinheit und aus einem Bedienfeld für die Feuerwehr. Dieses Bedienfeld ermöglicht den Einsatzkräften vor Ort die Steuerung der wichtigsten Funktionen. Über das Feld kann außerdem ganz genau festgestellt werden, welcher Melder das Signal ausgelöst hat.

Signal an Feuerwehr oder Wachdienst

Was konkret geschieht, wenn eine Brandmeldeanlage ein Feuer bemerkt, kann individuell bestimmt werden. Zum einen können Brandmeldeanlagen das Signal an eine durchgehend besetzte Feuerwehr-Leitstelle weiterleiten. Innerhalb weniger Minuten ist dann bereits ein Feuerwehr-Löschzug zum Einsatzort unterwegs. Möglich ist auch die interne Alarmierung – beispielsweise eines ständig besetzten Pförtnerbüros oder des Wachdienstes vor Ort. Das kann sinnvoll sein, um vor der Weiterleitung zur Feuerwehr kontrollieren zu können, ob ein Täusch- oder Fehlalarm vorliegt.

Die Alarmierung der Feuerwehr erfolgt meist über eine IP-Verbindung. Bei Ausfall dieser Verbindung wird entsprechend der Norm redundant eine alternative Möglichkeit genutzt. Das ist im Regelfall eine Verbindung über GSM-Mobilfunk.

Menschen frühzeitig warnen

Eine Brandmeldeanlage kann gleichzeitig auch einen Evakuierungsalarm auslösen. Mitarbeiter oder Bewohner werden dann durch ein Alarmsignal oder eine Durchsage gewarnt. Außerdem kann die BMA Aufzüge steuern und Rauchableitungseinrichtungen öffnen. Möglich ist auch die Auslösung einer Objektlöschanlage, etwa einer CO2-Löschanlage. Das alles geschieht automatisiert. Dadurch ist es möglich, die von einem Brand ausgehende Gefahr möglichst gering zu halten.

Brandmeldeanlage überlegt aufbauen

Mark Hochleitner

Wie eine BMA aufgebaut wird, das richtet sich ganz nach dem Gebäude, in dem sie installiert werden soll. Vor dem Einbau muss definiert werden, an welchen Stellen im Haus es strategisch sinnvoll ist, einen Brandmelder anzubringen. Handelt es sich um ein sehr großes Gebäude, dann werden meist mehrere Brandabschnitte oder Meldebereiche definiert.

Die eingetroffene Feuerwehr kann somit schnell feststellen, wo sich der Brandherd befindet. Dadurch können gezielte Löschvorgänge eingeleitet werden. Die Verbindung der Brandmelder untereinander erfolgt durch Schwachstromleitungen, die in den Kabelstrecken des Gebäudes verlegt werden.

Den Fachmann fragen

Die seit Ende 2003 gültige DIN 14675 legt fest, dass die Planung, Projektierung, Montage und Inbetriebnahme sowie Wartung einer Brandmeldeanlage nur von Firmen durchgeführt werden darf, die gemäß der DIN 14675 zertifiziert sind. Vertrauen Sie deshalb bei der Installation auf die Expertise von SEC-COM. Wir kennen uns aus mit Brandmeldesystemen, Einbruchmeldeanlagen und Videoüberwachung.

Bei allen Fragen hierzu informiert Sie das Team von SEC-COM gerne! Kontaktieren Sie uns noch heute.

Was Brandmeldeanlagen schützen:

- ✔ Personen oder Tiere im Gebäude
- ✔ Personen in der Nachbarschaft
- ✔ Sachwerte im Gebäude
- ✔ die Umwelt

Bauordnungsrecht regelt Einbaupflicht

Brandmeldeanlagen werden insbesondere in großen Gebäuden wie Flughäfen, Bahnhöfen, Universitäten, Schulen, Firmengebäuden, Fabrikhallen, Hotels, Altenwohnheimen oder Krankenhäusern eingebaut. Auch in größeren, modernen Wohnhäusern sind oftmals BMA installiert. Die Pflicht zum Einbau einer auf die Feuerwehr aufgeschalteten Brandmeldeanlage ist im Bauordnungsrecht im Rahmen von Sonderbauvorschriften geregelt. Gegebenenfalls kann die Bauaufsicht den Einbau einer Brandmeldeanlage mit der Baugenehmigung fordern. Angenehmer Nebeneffekt: Durch den Betrieb einer Brandmeldeanlage kann häufig eine reduzierte Versicherungsprämie der Gebäudeversicherung erreicht werden.

In Deutschland werden für die Planung bauordnungsrechtlich erforderlicher Brandmeldeanlagen im Regelfall die Anforderungen der DIN 14675 herangezogen. Von der Gebäudeversicherung akzeptierte Anlagen müssen den Anforderungen der VdS 2095 entsprechen.

„Brandschutz sollte jedes Unternehmen ernst nehmen. Dabei geht es nicht um Bürokratie, sondern um die Rettung von Menschen.“

Dirk Vespermann,
Technische Leitung
SEC-COM

Sie haben Fragen zu unseren Produkten oder Dienstleistungen?
Dann rufen Sie uns einfach an unter der Telefonnummer +49 2361 93220
oder senden uns eine E-Mail an info@sec-com.de

Die SEC-COM 2024 im Elektrizitätsmuseum

Mit Spannung in die Zukunft

Die SEC-COM 2024 im Deutschen Elektrizitätsmuseum Recklinghausen am 30. August setzt auch diesmal wieder auf informative Vorträge, spannende Diskussionen und die Möglichkeit zum Networking!

Zur SEC-COM 2024 im Deutschen Elektrizitätsmuseum Recklinghausen treffen sich am **Freitag, den 30. August** wieder Interessenten, Kunden, Partner und natürlich das SEC-COM Team. Technologieberatung, spannende Vorträge und die Möglichkeit zum Netzwerken stehen im Mittelpunkt. Besuchen Sie uns in der Zeit **von 9-17 Uhr**. Sind Sie (wieder) dabei? Wir freuen uns auf Sie!

Die Kernthemen auf der SEC-COM 2024 sind: KRITIS, die NIS-2-Richtlinie und Künstliche Intelligenz. Unsere Experten informieren Sie in Vorträgen und im persönlichen Gespräch über alle drei Themen, die für nahezu jeden Unternehmer und ITK-Verantwortlichen brandaktuell und relevant sind.

Zu KRITIS und NIS-2 erfahren Sie alle wichtigen Details zu den zu erfüllenden Verpflichtungen und – besonders wichtig bei NIS-2 – zum Zeitrahmen, der unbedingt eingehalten werden sollte. Das wichtigste Technikthema des Jahres ist aber Künstliche Intelligenz (KI), populär geworden durch das Tool Chat-GPT. Auf der SEC-COM 2024 erfahren Sie aus erster Hand, welche von uns angebotenen Lösungen bereits heute KI nutzen und mit welchen Tools Sie in naher Zukunft rechnen können. Machen Sie sich ein Bild davon, wie KI Ihren täglichen Workflow im Büro erleichtern und effizienter machen kann. Selbstverständlich informieren wir Sie auch über mögliche Risiken und über gesetzliche Bestimmungen, die es einzuhalten gilt.

Melden Sie sich heute noch an!

Informieren Sie sich auf der SEC-COM 2024 unverbindlich und ganz ohne Zeitdruck. Lassen Sie sich von der Museumsatmosphäre inspirieren, genießen Sie unsere Mittagssnacks, Kaffee und kühle Getränke.
Auch spontane Besuche sind möglich, aber Ihre Anmeldung vereinfacht unsere Planung und Vorbereitung sehr.

www.sec-com.de/sec-com-2024/

Fotos: Christiane Strunk

Unternehmensgruppe
SEC COM
Ihr **Systemhaus** für Kommunikation, Sicherheit und IT

„Der Preis ist das, was Sie bezahlen.
Wert ist das, was Sie bekommen.“

Warren Buffett, amerikanischer Unternehmer

2 x in NRW

SEC-COM Sicherheits- und Kommunikationstechnik GmbH

Am Stadion 117
45659 Recklinghausen
Fon: 0 23 61/93 22-0

SEC-COM Sicherheits- und Kommunikationstechnik Ostwestfalen GmbH
Karl-Schurz-Straße 19a
33 100 Paderborn
Fon: 0 52 51/8 74 98-0

www.sec-com.de