Foto: Stephan Franz Ferdinand Dinges

Kritische Infrastrukturen gilt es zu schützen – am besten bereits ab Perimeter. Doch ein Zaun allein reicht häufig nicht mehr. Die Lösungen sind vielfältig.

Zukunftsfähig sichern im Perimeter

Die Perimetersicherung wird immer wichtiger für den Schutz (Kritischer) Infrastrukturen und Gebäude, denn die Bedrohungslage wächst und verändert sich, worauf frühzeitig reagiert werden muss.

MARIE GRAICHEN

Angriffe und Attacken wandeln sich, diverse kriminelle Entwicklungen sind spürbar. Einerseits steigen physische Taten, andererseits strömen fortschrittliche und vor allem organisierte Angriffe aus dem Cyberraum in den Markt. Nach Angaben von Hikvision nehmen außerdem cyberphysische Angriffe zu, also kombinierte physische und digitale Methoden, um Sicherheitsmaßnahmen zu überwinden. Doch auch terroristische Bedrohungen auf öffentliche Einrichtungen und Infrastrukturen werden häufiger. Dabei wird deutlich, dass der technologische Fortschritt nicht nur neue Möglichkeiten für ganzheitliche Sicherheit mitbringt, sondern durch ihn auch neue Angriffsmöglichkeiten entstehen und das Risiko für Bedrohungen wächst. Das erfordert eine umfassende und anpassungsfähige Herangehensweise an die Perimetersicherung. Um den Herausforderungen begegnen zu können, sollten Lösungsanbieter und Unternehmen deshalb einige Schritte in die Wege leiten:

- Innovative Technologien implementieren, die sowohl physische als auch digitale Sicherheitsaspekte berücksichtigen.
- Proaktive Sicherheitsstrategien entwickeln, die kontinuierliche Risikoanalysen und Anpassungen beinhalten.
- In Schulungsprogramme investieren, um das Bewusstsein für potenzielle Bedrohungen zu schärfen

„Vernetzung wird das Thema der Zukunft sein."

Daniel Rekowski, Leiter Marketing und Vertrieb Perimeterschutz bei Zabag

Richtlinien für Regelung

Die neuen europäischen Richtlinien wie der Cyber Resilience Act (CRA) und die NIS-2-Richtlinie kommen laut Dahua zur richtigen Zeit, um Unternehmen und Bürger vor den Risiken der heutigen Bedrohungslage besser zu schützen. Für Lösungsanbieter und Unternehmen bedeutet dies jedoch wachsende Verantwortung. Sicherheit muss beispielsweise nachweisbar sein, das heißt, dass unter anderem Lieferanten ihre Cybersicherheitsstandards durch Zertifizierungen nachweisen müssen. Auch Lieferketten müssen stabil und widerstandsfähig gegen Schocks aufgestellt und abgesichert sein. Hier greifen Transparenzpflichten wie das Lieferkettengesetz (LkSG). Nicht zuletzt sind Investitionen in IT-Sicherheit und Produktentwicklung ein Muss, um langfristig wettbewerbsfähig bleiben.

Auswirkungen durch das Gesetz

Die Gesetze und Regelungen, die kommen, betreffen demnach auch den Markt für Perimetersicherung sowie dessen Kunden maßgeblich. „Vor allem das KRITIS-Dachgesetz zur Regelung Kritischer Infrastrukturen betrifft den Perimeterschutz. Die Referentenentwürfe beschreiben bereits Ansatzpunkte zum Schutz, bleiben jedoch sehr abstrakt und nach dem verstrichenen Umsetzungstermin Oktober 2024 wartet die Branche nunmehr auf die Einführung der Gesetzgebungen in nationales Recht", erklärt Daniel Rekowski, Leiter Marketing und Vertrieb Perimeterschutz von Zabag. Doch trotz Verzögerungen werden die Gesetze kommen und mit Kosten und Aufwänden verbunden sein. Hikvision fasst die Auswirkungen der kommenden Gesetzgebungen deshalb in mehrere Punkte zusammen:

- **Strengere Sicherheitsanforderungen:** Die neuen Regelungen fordern Unternehmen auf, robuste Sicherheitsmaßnahmen zu implementieren, um Kritische Infrastrukturen zu schützen. Dazu gehört auch die physische Sicherheit durch Perimeterschutz.
- **Dokumentationspflichten:** Unternehmen müssen Nachweise über ihre Sicherheitsmaßnahmen und -protokolle erbringen. Das bedeutet, dass alle Perimetersicherungsmaßnahmen dokumentiert und regelmäßig überprüft werden müssen.
- **Integration von Sicherheitslösungen:** Die Regelungen fördern die Verknüpfung von physischen und digitalen Sicherheitsmaßnahmen. Unternehmen müssen sicherstellen, dass ihre Perimetersicherungssysteme auch mit IT-Sicherheitslösungen zusammenarbeiten.
- **Schulungen für Mitarbeiter:** Mit den neuen Anforderungen steigt der Bedarf an Schulungen, um sicherzustellen, dass die Mitarbeiter die Sicherheitsprotokolle verstehen und umsetzen können. Die menschliche Komponente spielt eine entscheidende Rolle in der Sicherheitsarchitektur.
- **Regelmäßige Risikoanalysen:** Unternehmen sind verpflichtet, kontinuierlich Risikoanalysen durchzuführen, um potenzielle Schwachstellen in der Perimetersicherung zu identifizieren. Dies kann Investitionen in neue Technologien nach sich ziehen.
- **Verantwortung und Haftung:** Die neuen Gesetze schärfen das Bewusstsein für die Verantwortung von Unternehmen in Bezug auf ihre Sicherheitsinfrastruktur. Bei Nichterfüllung können rechtliche Konsequenzen drohen, was den Druck auf Unternehmen erhöht.
- **Innovationsförderung:** Die Notwendigkeit, die gesetzlichen Vorgaben zu erfüllen, könnte Innovationen im Bereich Perimeterschutz anstoßen. Unternehmen sind gefordert, neue Technologien und Lösungen zu entwickeln, um den Anforderungen gerecht zu werden.
- **Erhöhte Kosten:** Die Umsetzung der neuen Sicherheitsstandards kann mit höheren Kosten verbunden sein, sowohl durch Investitionen in Technologien als auch durch den Aufwand für Schulung und Dokumentation.

„Ein Blick in die DIN VDE V 0826-20 lohnt sich. Hierbei geht es explizit um Perimeter-Sicherungssysteme, um Perimeterschutz ideal zu planen."

Hauke Kerl-Kühn, Technischer Fachtrainer und Pre-Sales Engineer bei der Dahua Technology GmbH

„Die intensivere Risikobewertung wird in vielen Bereichen für Überraschungen sorgen – insbesondere bei der Abhängigkeit von Lieferanten und Dienstleistern. Das betrifft mitunter Aspekte wie die Lieferfähigkeit, wenn ein sicherheitskritisches System ausfällt und Ersatz schnell benötigt wird sowie das Thema Informationssicherheit. Konkret stellt sich die Frage: Wie „sicher" ist der Lieferant in puncto Informationssicherheit selbst?", ergänzt Hauke Kerl-Kühn, Technischer Fachtrainer und Pre-Sales Engineer bei Dahua.

Vernetzt im Perimeter

Die kommenden Anforderungen zeigen, dass Perimeterschutz inzwischen mehr ist als nur ein Zaun. Diverse Gewerke kommen für die umfassende Perimetersicherung zum Einsatz und müssen auch ineinandergreifen. „Neben der Hardware, also dem Hersteller von Schutzanlagen, kommen Gewerke des Tiefbaus, Architekten, Landschaftsplaner und Errichter zusammen. Neu sind die Zusammenspiele mit Anbietern von elektronischen Zutrittssystemen und Softwareanbieter, die alle Hardwarekomponenten miteinander kommunizieren und steuern lassen", erklärt Rekowski.

Die richtige Kombination hängt hierbei von einer ehrlichen Risikobewertung ab. Wichtige Faktoren, die je nach Einsatzbereich bewertet werden müssen, ▶

sind dabei unter anderem Widerstandsfähigkeit gegen Umwelteinflüsse und Manipulationsversuche, Benutzerfreundlichkeit und einfache Wartung. Auch die zentrale Verwaltung der Systeme sei laut dem technischen Fachtrainer und Pre-Sales Engineer von Dahua ein wichtiger Aspekt sowie Schulungen: „Ein effektives Perimeterschutzkonzept schließt auch organisatorische Maßnahmen ein, wie regelmäßige Übungen und Szenarientests mit allen Beteiligten. So wird sichergestellt, dass die Abläufe im Ernstfall klar sind und die Systeme ihre volle Wirkung entfalten können."

Entwicklungen im Perimeterschutz

Vernetzung wird immer mehr stattfinden. Das bestätigt auch der Leiter Marketing und Vertrieb Perimeterschutz von Zabag: „Vernetzung wird das Thema der Zukunft sein. Ein guter Perimeterschutz kann nur so gut sein wie die Möglichkeit der Steuerung und Überwachung durch den Betreiber. Die Reaktionszeit bei Aktionen gegen den Betreiber sind deshalb von immenser Bedeutung." Deshalb sind neuartige Technologien für mehr Schutz und Sicherheit unabdingbar, doch müssen diese auch sicher in sich selbst sein, wie Kerl-Kühn beschreibt: „Nicht jedes Gerät kann mit allem vernetzt sein, da dies die Sicherheit gefährden könnte. Die Vernetzung der Zukunft wird daher ‚klug' gestaltet: Perimetersicherheitslösungen müssen so konfiguriert sein, dass sie verdächtige Aktivitäten erkennen und Angriffe frühzeitig detektieren können." Neben intelligenter Vernetzung wird sich die Perimetersicherung jedoch auch in weiteren Bereichen fortentwickeln. Laut Christian Kastner, Teamleader Pre-Sales DACH von Hikvision, wird Künstliche Intelligenz und maschinelles Lernen vermehrt zum Einsatz kommen, wenn es darum geht, Verhaltensmuster zu erkennen.

> „Eine moderne Perimetersicherung kombiniert technische Top-Produkte mit organisatorischer Weitsicht, setzt auf bewährte Standards und Normen und bleibt zugleich flexibel und kosteneffizient."
>
> **Hauke Kerl-Kühn,** Technischer Fachtrainer und Pre-Sales Engineer bei der Dahua Technology GmbH

Außerdem werden IoT-Geräte integriert werden, um durch vernetzte Kameras und Sensoren eine verbesserte Überwachung und Analyse von Sicherheitsdaten zu gewährleisten. Auch Cloud-basierte Lösungen wirken auf die Entwicklung im Markt ein, da sie eine zentrale Plattform für die Verwaltung und Analyse von Sicherheitsformen darstellen, die Skalierung und die Integration neuer Technologien erleichtert. Das sorgt für flexiblere Reaktionen auf die sich verändernden Angriffsszenarien. Durch die Analyse von Daten können potenzielle Bedrohungen besser vorhergesagt werden, sodass Unternehmen proaktive Maßnahmen ergreifen können. All das ist möglich, ohne vor Ort sein zu müssen, da Sicherheitsmanager die Systeme zunehmend über mobile Anwendungen überwachen und steuern können, was die Flexibilität und Reaktionsgeschwindigkeit erhöht. „Unternehmen werden im Zuge dessen auch enger zusammenarbeiten, um Informationen über Bedrohungen und Sicherheitslösungen auszutauschen, was den Wissenstransfer und die Entwicklung von Best Practices fördert", ergänzt Kastner, was die Effizienz der Perimetersicherung erhöht und eine umfassende Sicht auf die Sicherheitslage ermöglicht, um schnellere und fundierte Entscheidungen zu treffen. „Eine moderne Perimetersicherung kombiniert technische Top-Produkte mit organisatorischer Weitsicht, setzt auf bewährte Standards und Normen und bleibt zugleich flexibel und kosteneffizient", erklärt Kerl-Kühn. ■

Perimetersicherung am Zahn der Zeit

Moderne Perimetersicherung muss verschiedene Anforderungen erfüllen, um einen effektiven Schutz zu gewährleisten. Folgende Punkte sind wesentlich:

1. **Echtzeitüberwachung**: Systeme sollten kontinuierlich den Perimeter im Blick haben, um potenzielle Bedrohungen sofort zu erkennen und darauf zu reagieren.
2. **Technologische Integration**: Eine Kombination aus physischer Sicherheit (wie Zäune und Mauern) und digitalen Lösungen (wie Kameras und Sensoren) ist entscheidend. Diese Systeme sollten miteinander kommunizieren, um eine umfassende Sicherheitslage zu schaffen.
3. **Automatisierte Reaktionen**: Bei der Erkennung von Bedrohungen sollten automatisierte Maßnahmen ergriffen werden können, beispielsweise durch das Aktivieren von Alarmen oder das Senden von Benachrichtigungen.
4. **Flexibilität und Skalierbarkeit**: Sicherheitslösungen sollten anpassbar sein, um verschiedenen Sicherheitsanforderungen gerecht zu werden und neue Technologien problemlos integrieren zu können.
5. **Benutzerfreundlichkeit**: Die Bedienung der Systeme muss intuitiv sein, damit das Sicherheitspersonal schnell reagieren kann. Klare Schnittstellen und Schulungen sind hierbei wichtig.
6. **Schutz der Daten**: Da viele Systeme vernetzt sind, ist der Schutz vor Cyberangriffen entscheidend. Dazu gehören regelmäßige Updates und Sicherheitsüberprüfungen.
7. **Analytische Fähigkeiten**: Systeme sollten in der Lage sein, Daten zu analysieren und Muster zu erkennen, um proaktive Sicherheitsstrategien zu entwickeln und Risiken frühzeitig zu identifizieren.
8. **Notfallkommunikation**: Effektive Kommunikationssysteme sind entscheidend, um im Ernstfall schnell Informationen weiterzugeben und Maßnahmen zu koordinieren.
9. **Regelmäßige Wartung**: Um die Effizienz und Sicherheit zu gewährleisten, sollten Systeme regelmäßig gewartet und aktualisiert werden.

Quelle: Hikvision