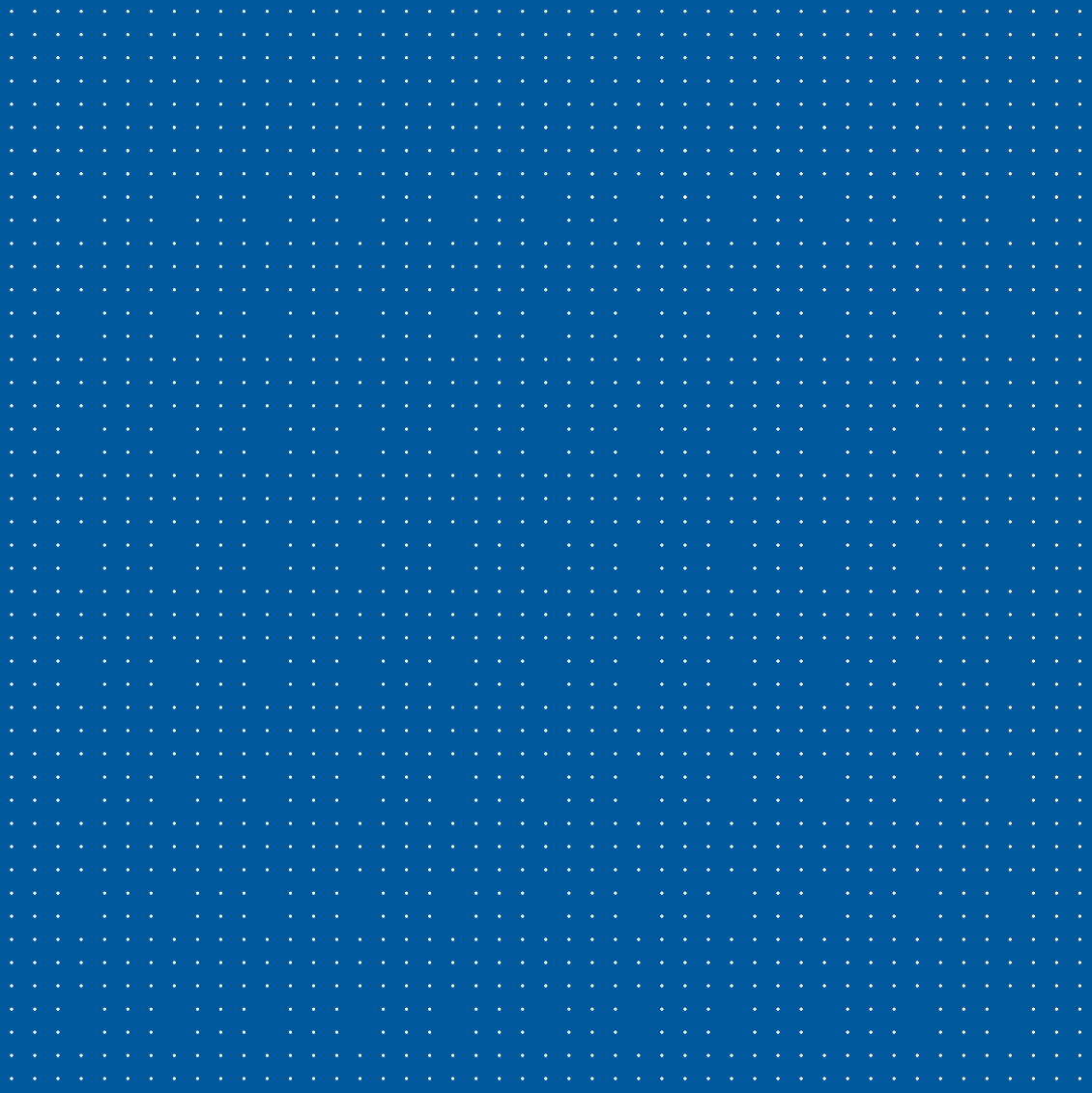
Verbesserter Schutz vor Cyberangriffen

Schutz gegen Cyberkriminalität



Genetec™

Die wachsenden Risiken einer vernetzten Welt

Cyberkriminalität kann zu erheblichen Störungen der Aktivitäten von Organisationen und Behörden führen. Im Jahr 2017 hat eine große Ransomware-Attacke, bekannt als WannaCry, Menschen und Organisationen auf der ganzen Welt betroffen. Ziel des Ransomware-Angriffs war gängige, aber veraltete Software. Durch den Angriff waren mehr als 230.000 Computer in 15 Ländern gesperrt. Im Gegenzug für die Aufhebung der Sperre verlangten die Urheber der Ransomware die Zahlung enormer Summen. In vielen Krankenhäusern wurden Patientendatensätze verschlüsselt, weswegen Operationen abgebrochen werden mussten und das Leben der Patienten in Gefahr geriet.

Von Erfolgen wie bei WannaCry fühlten sich Cyberkriminelle ermutigt, den Umfang der Angriffe auf private Sicherheitskameras auszuweiten und auf Live-Videodaten zuzugreifen. Bei einigen dieser Angriffe werden einfache Schwachstellen ausgenutzt, etwa die Tatsache, dass die Standardpasswörter des Herstellers nicht geändert wurden. Andere Angriffe hingegen sind deutlich ausgereifter und komplexer. Ganz gleich, ob auf der Arbeit oder zu Hause: Fremde vom Zugriff auf Kameras abzuhalten, ist keine unkomplizierte Angelegenheit mehr.

Durch die umfassendere Vernetzung von Systemen über das Internet kann ein unsicheres Gerät zum Einfallstor für den Zugriff auf die Daten Ihrer Organisation und auf vertrauliche Informationen werden. Durch die Absicherung Ihrer physischen Sicherheitssysteme tragen Sie auch zur Absicherung aller anderen Systeme und der Informationen im Netzwerk bei. Hierfür benötigen Sie eine neue Herangehensweise mit einer in die Tiefe gehenden Verteidigungsstrategie.

Eine in die Tiefe gehende Verteidigungsstrategie entwickeln

Wie bei allen vernetzten Entitäten können Sicherheitssysteme zur Zielscheibe werden. Das Hacken eines Sicherheitssystems kann auf verschiedene Weisen erfolgen, beispielsweise durch Brute-Force-, Packet-Sniffing- oder Man-in-the-Middle-Angriffe. In einigen Fällen sind Cyberkriminelle in der Lage, Kommunikation „abzuhören“ und zu verändern, ohne dass die Kommunikationsteilnehmer Zweifel an der Sicherheit ihres Systems bekommen. Der Vielfalt von Angriffsstrategien muss eine ebenso große Vielfalt an Verteidigungsebenen entgegengesetzt werden.

Genetec bietet sichere, geprüfte und konforme Lösungen, mit denen Sie die Daten von allen Personen ohne Einschränkung der Sicherheit schützen können. Wir helfen Ihnen dabei, mehrere unterschiedliche Verteidigungslinien zum Schutz vor bekannten und neuen Bedrohungen und zur Sicherheit Ihrer Umgebung zu ziehen. Die einzelnen Linien werden auch als in die Tiefe gehende Verteidigungsstrategie für Cybersicherheit bezeichnet. Für den Schutz von Daten, die von unserem einheitlichen Sicherheitssystem für Management, Analyse und Speicherung erfasst werden, werden starke Methoden für Verschlüsselung, Authentifizierung und Autorisierung eingesetzt.

Von der physischen Sicherheit zur Cybersicherheit

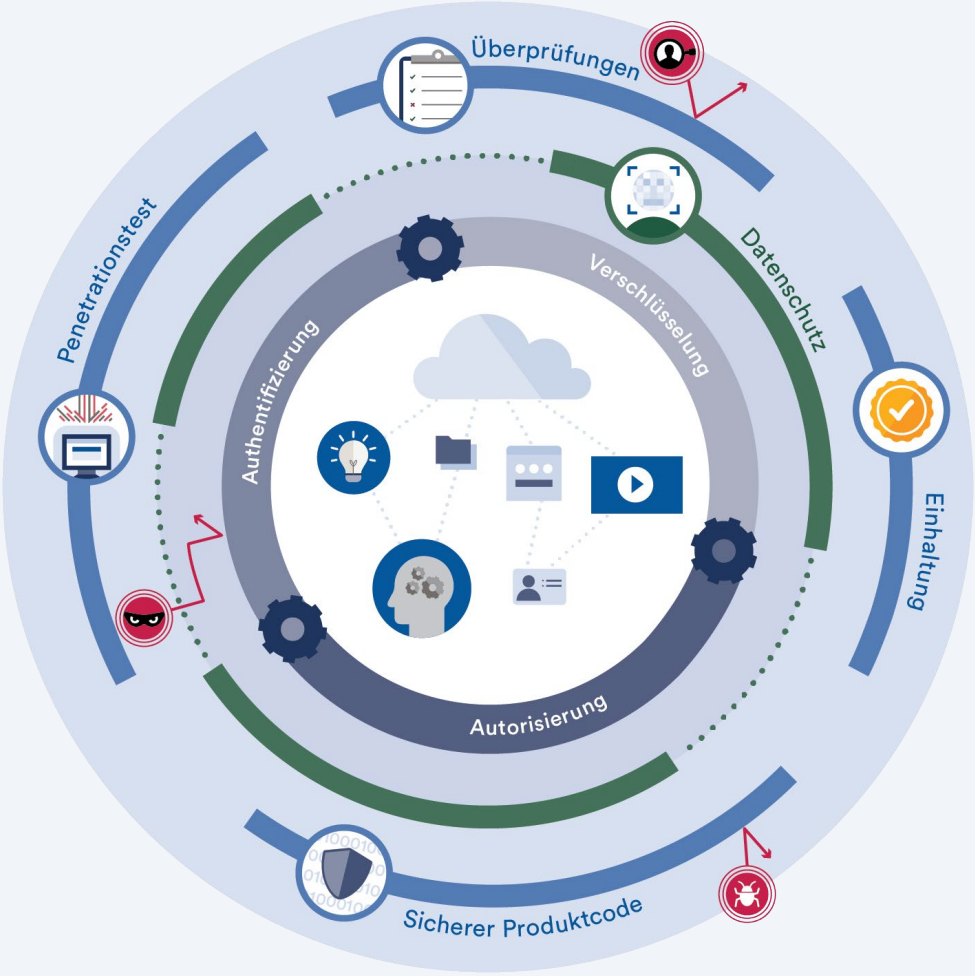
Kameras, Türsteuerungen und andere physische Sicherheitssysteme und -geräte sind intelligenter und leistungsstärker als jemals zuvor. Sie sind sowohl in öffentliche als auch in private Netzwerke integriert und in zunehmendem Maße vernetzt. Das erleichtert die Verwaltung, beschleunigt die Kommunikation und erweitert die gemeinsame Nutzung von Daten. Vor allem aber können Sicherheitsexperten auf diese Weise für die Sicherheit von Menschen und Organisationen sorgen.

Die stärkere Vernetzung bringt jedoch nicht nur Vorteile mit sich. Aufkommende Cyberbedrohungen, Gefahren und kriminelle Aktivitäten führen auch zu neuen Sicherheitslücken und -risiken.

Eine schlecht geschützte Kamera, unverschlüsselte Kommunikation zwischen Server und Client-Anwendung oder veraltete Firmware sind Einfallstore für Cyberkriminelle. Hieraus lässt sich eine Schlussfolgerung ziehen: Sicherheitssysteme dürfen nicht mehr allein auf physische Bedrohungen ausgerichtet sein.

Aus diesem Grund halten wir es für unerlässlich, eine Sicherheitsstrategie zum Schutz des Systems gegen physische Bedrohungen und Cyberbedrohungen einzurichten. Mit unseren Lösungen erhalten Sie die Instrumente an die Hand, die Sie für ein sicheres und konformes System benötigen. Auf einen Aspekt reduzierte Herangehensweisen helfen nicht weiter. Daher bestehen die Lösungen aus mehreren Verteidigungsebenen wie Verschlüsselung, Multi-Faktor-Authentifizierung und Autorisierung. Von den Geräten bis hin zum Datenspeicher vor Ort und in der Cloud helfen wir Ihnen dabei, sich vor neuen Bedrohungen zu schützen und für die Sicherheit der Daten und der Arbeitsabläufe zu sorgen.

Vorausschauende Planung und umfassende Praxis



Die einzelnen Ebenen unseres in die Tiefe gehenden Sicherheitskonzepts schützen Sie vor einer Reihe von Bedrohungen.

Auf geprüfte und konforme Lösungen setzen

Wir arbeiten eng mit internationalen Verbänden zusammen, damit unsere Lösungen Branchenstandards erfüllen und sich an den neuesten Best Practices für Cybersicherheit orientieren. An unseren Produkten werden regelmäßig Durchdringungstests und Prüfungen durchgeführt, mit denen eine vollständige Bewertung der Integrität unserer Lösungen möglich wird.

Den richtigen Personen Informationen zugänglich machen

Wenn Sie Ihre Daten schützen möchten, dürfen Sie sich nicht nur auf Bedrohungen von außen konzentrieren. Durch die engere Integration und Zusammenarbeit der einzelnen Komponenten unserer Sicherheitssysteme hat sich die Zahl der Pfade für den Zugriff auf vertrauliche Daten vervielfacht. Aus diesem Grund müssen Sie kontrollieren, wer Ihre Daten ansehen und was derjenige damit tun kann.

Der erste Schritt besteht in der Verwendung starker Authentifizierungsmethoden, damit keine Unbefugten auf das System zugreifen können. Dadurch wird verhindert, dass Videos und Daten in die falschen Hände geraten. Nach der Authentifizierung besteht der nächste Schritt darin, per Autorisierung zu steuern, wer auf welche Bereiche Ihres Sicherheitssystems zugreifen kann. So können Sie die Aktivitäten im System einschränken, indem sie Gruppen oder Einzelpersonen Zugriffsrechte auf Ressourcen, Daten oder Anwendungen gewähren und definieren, wie Benutzer diese Ressourcen einsetzen können.

Abschirmung vor neugierigen Blicken

Wir helfen Ihnen auf verschiedene Weisen dabei, Ihre Daten vor böswilligen Angriffen zu schützen. Beim verbesserten Schutz vor Cyberangriffen geht es um den Schutz sämtlicher Aspekte ihres physischen Sicherheitssystems, das Kommunikation, Server und Daten umfasst.

Videos und Daten, die in unserem System angezeigt und gespeichert werden, sowie die Kommunikation mit Genetec-Hardware werden vollständig verschlüsselt. Wir schützen auch die Kommunikation zwischen unserer Software und Peripheriegeräten, sowie der Cloud. Auf diese Weise wird verhindert, dass Unbefugte, sollten sie Zugriff erlangt haben, die Daten nutzen können, weil ihnen der Entschlüsselungsschlüssel fehlt.

Datenschutz für alle

Die Überwachung von Personen und Geräten erfordert häufig die Erfassung personenbezogener Daten und die Überwachung öffentlicher Räume. Um Vorschriften einzuhalten und öffentlichen Erwartungen gerecht zu werden, muss der Zugriff auf personenbezogene Daten und das Bildmaterial kontrolliert werden. Mit unserem Konzept des integrierten Datenschutzes sorgen wir dafür, dass Sie sich nicht zwischen dem Schutz der Daten und der physischen Sicherheit von Personen entscheiden müssen. Unsere Produkte helfen Ihnen dabei, den Zugriff auf vertrauliche Daten zu verwalten und die Identität aller auf Video aufgezeichneten Personen zu schützen.

Wir sorgen dafür, dass Sie die vollständige Kontrolle über Ihre Daten haben, sodass Sie Ihre Schutzmethoden und Prozesse an die Vorschriften wie etwa die europäische Datenschutz-Grundverordnung (DSGVO) anpassen sowie vor allem Vertrauen zu Ihren Kunden aufbauen können.

Der Faktor Mensch

Die Technologie ist zwar äußerst wichtig, wenn es darum geht, Ihre Organisation vor kriminellen Cyberaktivitäten zu schützen, doch ein weiterer Faktor spielt ebenfalls eine zentrale Rolle: Ihre Mitarbeiter. Die beste Verschlüsselung ist nutzlos, wenn Ihr System mit schwachen oder entschlüsselten Passwörtern eine offene Flanke bietet. Aus diesem Grund müssen die richtigen Prozesse implementiert und die richtigen Schulungsprogramme umgesetzt werden. Die Mitarbeiter benötigen Schulungen zu den bewährten Vorgehensweisen der IT und zu den Social-Engineering-Techniken, mit denen sie potenziell konfrontiert werden. Beispielsweise lassen sich Cyberisiken schon durch die Beachtung einfacher Tipps zur Erstellung von Passwörtern und das Wissen darüber, woran sich Phishing-E-Mails von legitimer Kommunikation unterscheiden, reduzieren.

Vertrauen aufbauen

Als Anbieter von Sicherheits-, Betriebs- und Business-Intelligence-Lösungen helfen wir Ihnen beim Schutz Ihres Unternehmens. Wir arbeiten unermüdlich daran, Sie über neue Bedrohungen zu informieren und Ihnen beim Schließen von Sicherheitslücken zu helfen. Wir werden auch weiterhin in Kooperation mit unseren Kunden und Partnern Lösungen bereitstellen, die heute und in Zukunft bestmöglichen Schutz bieten.

Weitere Informationen zu unseren Konzepten und zum Schutz Ihres Systems finden Sie unter **genetec.com/trust**.

Genetec Inc.
genetec.com/standorte
info@genetec.com
@genetec