Deutschland

Genetec Deutschland GmbH
De-Saint-Exupéry-Straße 10
60549 Frankfurt am Main
Deutschland

T +49 695 06028 255

Pressemitteilung

KI verstärkt Cyberrisiken: Genetec rät dringend zu strengerem Management von Nutzerprofilen und Berechtigungen bei vernetzten physischen Sicherheitssystemen

Passwortänderungen allein reichen nicht mehr aus, um physische Sicherheitsumgebungen zu schützen, warnt Genetec im Vorfeld des World Password Day

FRANKFURT, 06. Mai 2026 – Genetec Inc. („Genetec"), der weltweit führende Anbieter von Software für die physische Sicherheit in Unternehmen, fordert Organisationen dazu auf, die Kontrolle für Authentifizierungs- und Zutrittsinformationen in vernetzten physischen Sicherheitssystemen zu verstärken. Hintergrund ist, dass KI das Ausmaß und die Komplexität von Cyberbedrohungen weiter erhöht.

KI-gestützte Tools verstärken Angriffe auf Authentifizierungsdaten und Passwörter: Attacken erfolgen schneller, in größerem Ausmaß und mit mehr Präzision. In Unternehmen, die vernetzte Kameras, Zutrittskontrollsysteme, Server und Cloud-Dienste einsetzen, können schwache oder unzureichend verwaltete Zutrittsdaten und Passwörter sensible Betriebsabläufe gefährden und neue Angriffswege in die Unternehmensinfrastruktur eröffnen. Dazu gehören auch die Passwörter, die für die direkte Verbindung mit den Geräten verwendet werden. Diese werden oft übersehen, können aber bei unsachgemäßer Verwaltung einen direkten Angriffspunkt bieten. In diesem Umfeld reicht es nicht mehr aus, sich auf regelmäßige Änderungen von Passwörtern oder einfache Cybersicherheitsmaßnahmen zu verlassen.

„KI verändert Tempo und Ausmaß von Cyberrisiken", sagt Mathieu Chevalier, Principal Security Architect bei Genetec Inc. „Angreifer können heute schneller agieren. Sie nutzen KI, um sich als Personen auszugeben, Social-Engineering-Angriffe gezielt durchzuführen, Schwachstellen in großem Umfang aufzudecken und der Erkennung zu entgehen. Unternehmen müssen daher den Zutritt und die Identitäten auf ihre gesamten Systeme

aktiv steuern, statt Kontrollen einmalig einzurichten und darauf zu hoffen, dass sie dauerhaft greifen."

Die Risiken betreffen bereits Unternehmen, die physische Sicherheitssysteme betreiben. Die aktuelle Studie „Genetec Enterprise Physical Security in the Cloud Era", die auf Erkenntnissen von mehr als 7.300 Fachleuten für physische Sicherheit weltweit basiert, zeigt, dass 58,7 Prozent der Unternehmen einen Anstieg von Phishing- und Smishing-Angriffen verzeichnen und 41 Prozent einen Anstieg der physischen oder Cyber-Vorfälle insgesamt. Social Engineering wird von 43,5 Prozent als meist genutzter Angriffsvektor genannt.

Stärkung der Identitäts- und Zutrittskontrollen

Unternehmen sollten voreingestellte, standardisierte und gemeinsam genutzte Zutrittsdaten und Passwörter abschaffen. Um häufige Schwachstellen für Angriffe zu beseitigen, wird empfohlen, eine starke Authentifizierung wie Passkeys und die Multi-Faktor-Authentifizierung (MFA) einzusetzen. Dies muss sich auch auf Geräte erstrecken. Statische Passwörter sollten nach Möglichkeit durch eine zertifikatsbasierte Authentifizierung ersetzt werden. Außerdem sollten die Verantwortlichen eine zentralisierte Verwaltung sowie eine regelmäßige Änderung der Anmeldedaten sicherstellen.

Engere Koordination zwischen IT- und physischen Sicherheitsteams

Die Zusammenarbeit von IT- und physischen Sicherheitsteams trägt dazu bei, einheitliche Sicherheitsstandards anzuwenden, den Überblick über Zutrittsrisiken zu verbessern und die Reaktion auf Vorfälle zu koordinieren. Da physische Sicherheitssysteme zunehmend mit Unternehmensnetzwerken verbunden sind, können Organisationen durch eine funktionsübergreifende Koordination ihre Schwachstellen besser identifizieren und effektiver auf Angriffe reagieren, die auf Zutritts- und Berechtigungsdaten abzielen.

Governance beim Management physischer Sicherheitssysteme priorisieren

Organisationen sollten ihre physische Sicherheitsinfrastruktur mit derselben Sorgfalt betreiben wie andere geschäftskritische Systeme. Dazu gehören die regelmäßigen Überprüfungen der Zutritte und Zugriffe, kontrollierte Updates und Partnerschaften mit vertrauenswürdigen Technologieanbietern, die langfristige Sicherheit, Transparenz und operative Ausfallsicherheit gewährleisten.

Weitere Informationen darüber, wie Unternehmen Cyberrisiken in vernetzten physischen Sicherheitsumgebungen bewältigen, erfahren Sie in der Genetec-Studie „Enterprise Physical Security in the Cloud Era“.

Über Genetec

Genetec ist ein global agierendes Technologieunternehmen, das seit über 25 Jahren die physische Sicherheitsbranche entscheidend prägt. Mit dem Lösungsportfolio von Genetec können Unternehmen, Behörden und Kommunen weltweit Menschen und Betriebsanlagen sichern und gleichzeitig die Privatsphäre des Einzelnen schützen sowie betriebliche Effizienz realisieren.

Genetec bietet die weltweit führenden Produkte für Videomanagement, Zutrittskontrolle und ALPR, die alle auf einer offenen Architektur aufbauen und deren Kernstück Cybersicherheit ist. Das Portfolio des Unternehmens umfasst zudem Lösungen für die Einbruchserkennung, Sprechanlagen und das digitale Beweismanagement.

Genetec hat seinen Hauptsitz in Montreal, Kanada, und betreut seine mehr als 42.500 Kunden über ein umfangreiches Netzwerk von akkreditierten Vertriebspartnern und Beratern in über 159 Ländern.

Weitere Informationen über Genetec gibt es unter www.genetec.de.

Pressekontakt:

Patrick Rothwell
Miriam Seyd
Fink & Fuchs AG
Tel.: +49 611 74131-0
E-Mail: genetec@finkfuchs.de