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

Tel.: +49-(0) 69 506028-255
E-Mail: SalesDACH@genetec.com
genetec.de

Genetec: Die Top-5-Trends für physische Sicherheit 2021

- **Innovative neue Anwendungen für vorhandene Sicherheitstechnologien**
- **Fokus auf Datenschutz**
- **Wachsende Cybersecurity-Risiken**
- **Zunehmende Überprüfung von Anbietern**
- **Einführung von Hybrid-Cloud-Modellen**

Frankfurt, 18. Januar 2021 — Genetec, führender Technologie-Anbieter für vereinheitlichtes Sicherheitsmanagement, öffentliche Sicherheit und Business Intelligence, sieht für das Jahr 2021 die fünf folgenden zentralen Trends für den Bereich physische Sicherheit.

Innovative Sicherheitslösungen auch für die Zeit nach COVID-19

Unternehmen müssen kreativ bleiben, wenn es darum geht, vorhandene Sicherheitssysteme in ihren Einrichtungen einzusetzen, zu aktualisieren und für neue Einsatzbereiche nutzbar zu machen. Physische Sicherheit muss über traditionelle Anwendungen hinaus breiter gedacht werden, um Mehrwert zu liefern. In den letzten Monaten konnte man bereits eindrückliche Beispiele für diese Kreativität sehen. Viele Unternehmen haben sich im Rahmen der Pandemie den neuen Herausforderungen gestellt und ihre physische Sicherheitstechnologie als strategisches Werkzeug im Kampf gegen COVID-19 genutzt. Gerade mit Blick auf die besonderen Probleme, die diese schwierige aktuelle Situation mit sich bringt, steht die physische Sicherheit besonders im Fokus. Das wird dazu führen, dass zentrale, vereinheitlichte Sicherheitssysteme auch nach COVID-19 zukünftig verstärkt als strategisches Unternehmenstechnologie eingesetzt werden.

Der Schutz der Privatsphäre gewinnt weiter an Bedeutung

Um Menschen zu schützen, haben viele Unternehmen nach Ausbruch der Pandemie rasch Lösungen z.B. für Fiebererkennung implementiert. Dabei fehlte häufig die Zeit, mögliche Auswirkungen auf die Privatsphäre zu berücksichtigen. Die Datenschutzbedenken der Öffentlichkeit im Zusammenhang mit der COVID-19-Kontaktverfolgung und andere soziale Herausforderungen werden die Sicherheitsbranche dazu zwingen, sich vermehrt mit dem Datenschutz auseinanderzusetzen und adäquate Lösungen zu finden. Der Datenschutz

wird die Entwicklung neuer Technologien dabei nicht behindern, sondern wird vielmehr ein verantwortungsvolles und innovatives Lösungsdesign fördern und zukunftsorientierte, ethische Entwickler werden „Privacy-by-Design"-Methoden übernehmen. Der Datenschutz wird proaktiv in das Design und den Betrieb von IT-Systemen, die Netzwerk-Infrastruktur und Geschäftsprozessen eingebettet – von der ersten Code-Zeile bis zu den für die Partnerschaft und Integration ausgewählten Drittanbietern. Für die physische Sicherheitsbranche bedeutet dies, dass Kunden nicht zwischen dem Schutz der Privatsphäre und der Gewährleistung physischer Sicherheit wählen müssen. Datenschutz sollte als Standard voreingestellt sein. Entwickler von Sicherheitslösungen, die das Thema Datenschutz ernst nehmen, werden hier deutliche Vorteile haben, vor allem aber das Vertrauen ihrer Kunden gewinnen.

Cybersecurity-Risiken werden weiter zunehmen

Cybersecurity ist seit einiger Zeit ein wichtiges Thema und wird es leider auch im Jahr 2021 bleiben. Schulen, Krankenhäuser und auch Privatunternehmen und Behörden waren im vergangenen Jahr von einer steigenden Anzahl von Cyberangriffen betroffen. Allein im dritten Quartal 2020 gab es im laut Trend Micro fast vier Millionen Bedrohungen durch E-Mails und mehr als eine Million Zugriffe auf bösartige Websites im Zusammenhang mit COVID19.

Der kurzfristige Umstieg auf Homeoffice trug stark zu dieser Entwicklung bei. Viele Unternehmen mussten quasi über Nacht umsteigen, um den Geschäftsbetrieb aufrechterhalten und gleichzeitig Unternehmensressourcen zu schützen. Aufgrund dieser Verlagerung gibt es eine abgegrenzte, sichere IT-Umgebung jedoch nicht mehr. Schulen, Unternehmen und öffentliche Einrichtungen müssen Maßnahmen implementieren, um ihre Cybersicherheit zu erhöhen, andernfalls riskieren sie den Verlust geistigen Eigentums oder sensibler Unternehmensdaten sowie persönlicher Informationen. Entscheidend wird es sein, vertrauenswürdige Anbieter auszuwählen und Sicherheitslösungen einzusetzen, die über mehrere Sicherheitsebenen verfügen. Verschlüsselung, Multi-Faktor-Authentifizierung und Passwortmanagement sind dabei die erste Verteidigungslinie. Darüber hinaus sind der Zugriff auf Cyberrisiko-Scoringsysteme, Warnhinweise auf Systemschwachstellen und automatisierte Hinweise auf Firmware- und Hardware-Updates erhebliche Vorteile in einem Umfeld mit erhöhtem Risiko.

Stärkerer Fokus auf vertrauenswürdige Partner

Physische Sicherheitstechnologie ist mittlerweile ein integraler Bestandteil der IT-Strategie eines Unternehmens. Die eingesetzte Sicherheitsinfrastruktur wird deshalb nun erfreulicherweise ebenso gründlich geprüft wie andere IT-Bestandteile. Weltweit raten

die ersten Regierungen vom Einsatz bestimmter Lösungen mit dem Hinweis auf mögliche Vertrauensdefizite und Sicherheitslücken ab. Anwender, vor allem aus dem Unternehmensumfeld, nehmen sich heute bereits deutlich mehr Zeit, um Hersteller, Lieferanten und Distributoren, mit denen sie zusammenarbeiten, genau zu überprüfen. Dazu gehören auch Fragen nach dem Umgang mit neuen Bedrohungen, wie offen Schwachstellen eigener Produkte sowie der Produkte aus dem Partnerökosystem adressiert werden und wie ihre Datenschutzrichtlinien aussehen. Anbieter von physischen Sicherheitslösungen müssen künftig höhere Anforderungen im Rahmen des Beschaffungsprozesses erfüllen, um als vertrauenswürdiger, verlässlicher Anbieter eingestuft zu werden.

Steigende Nachfrage nach hybriden Cloud-Lösungen

Das Markforschungsinstitut Forrester geht in seinem aktuellen Bericht „Predictions 2021: Cloud Computing Powers Pandemic Recovery“ davon aus, dass der Markt für Public-Cloud-Infrastruktur im Jahr 2021 weltweit um 35 Prozent auf ein Marktvolumen von 120 Milliarden US-Dollar wachsen wird. Die digitale Transformation während der Pandemie wurde durch die zunehmende Online-Nutzung und Homeoffice deutlich beschleunigt. Sicherheitsfachleute sollten daher dem Beispiel der IT-Abteilungen folgen, um auch in Zukunft gut aufgestellt zu sein. Im kommenden Jahr werden physical Security-Verantwortliche vermehrt die klare Trennung zwischen Cloud und On-Premise aufgeben und auf hybride Lösungen im Rahmen ihrer physischen Sicherheitsinfrastruktur umsteigen. So lassen sich spezialisierte Systeme und Anwendungen in der Cloud implementieren, gleichzeitig können aber bestehende On-Premise-Systeme beibehalten werden.

Mit einem hybriden Cloud-Ansatz sind Sicherheitsverantwortliche flexibler und haben mehr Möglichkeiten, um Skalierbarkeit, Redundanz und Verfügbarkeit ihrer Systeme zu verbessern und an die steigenden Anforderungen ihres Unternehmens anzupassen. Darüber hinaus können sie schneller auf neue Technologien migrieren, Hardware reduzieren, die Cybersicherheit erhöhen und Kosten senken. Cloud-Angebote sollten als zentrale Option angesehen werden, um sich schnell an Veränderungen anpassen und Betriebskontinuität gewährleisten zu können.

Über Genetec

Genetec ist ein innovatives Technologieunternehmen mit einem breiten Lösungsportfolio für Sicherheit, Information und operativen Betrieb von Unternehmen und Organisationen. Die zentrale Lösung Security Center vereinheitlicht IP-basierte Videoüberwachung, Zutrittskontrolle, Nummernschilderkennung, Kommunikation und Analyse auf einer einzigen Plattform. Genetec

entwickelt darüber hinaus Cloud-Lösungen und -Services. Sie erhöhen die Sicherheit und tragen dazu bei, dass Regierungsverantwortliche, Unternehmen, Verkehrsbetriebe sowie Städte und Gemeinden, in denen wir leben, neue Erkenntnisse über ihre Betriebsabläufe erhalten. Das Unternehmen mit Sitz in Montreal, Kanada, wurde 1997 gegründet. Genetec betreut Kunden weltweit mit einem umfangreichen Netzwerk aus zertifizierten Vertriebspartnern, Systemintegratoren und Beratern in über 80 Ländern.

Weitere Informationen: www.genetec.de

Pressekontakt
Tobias Merklinghaus
BSK Becker+Schreiner Kommunikation GmbH
Tel.: +49 (0) 2154 8122-15
E-Mail: merklinghaus@kommunikation-bsk.de