Global Headquarters

Genetec Inc.
2280 Alfred Nobel Blvd.
Montreal, Quebec H4S 2A4
Canada
T: +1 514.332.4000

Media Alert

Genetec cautions public sector to harden physical security systems against digital threats in light of rising cyberattacks

Protecting cameras and access control systems, integrating IT and security teams can reduce risk

MONTRÉAL, April 14, 2022 — Following a pandemic-exacerbated rise in data breaches and ransomware attacks, Genetec Inc. ("Genetec"), a leading technology provider of unified security, public safety, operations, and business intelligence solutions, guided public sector organizations on how to reduce cyber vulnerabilities of physical security systems that are often overlooked.

IP security cameras and other security devices were put in place to protect people, assets, and environments. But the same network connectivity that enables organizations to monitor operations and update software remotely presents a path into the network for cyber criminals. If they are not sufficiently modern or properly shielded, they can pose significant risk to cybersecurity. An attack that originates in a camera or door controller can find its way through the network to block access to critical applications, lock files for ransom, and steal personal data.

Justin Himelberger, Enterprise Systems Business Development Manager for US Federal and DOD at Genetec Inc., said, "Because these systems – video surveillance, access control, alarms, communications, and more – are increasingly connected to networks and IT infrastructure, they can be quite vulnerable. With the number of cyberattacks increasing around the world, it is becoming clear that government organizations must be more stringent than ever about cybersecurity in their own organizations and throughout their supply chains."

A step organization can take immediately is making sure each device, as well as the servers used for storing data and hosting monitoring consoles, has the latest version of firmware and software recommended by the manufacturer. Changing default passwords and establishing a process to change them frequently is a critical practice. Improving network design to segment older devices can also help reduce the potential for crossover attacks.

Assessing and Preventing Vulnerabilities

To determine the risk of physical security systems, Genetec recommends organizations conduct a posture assessment, creating and maintaining an inventory of all network-connected devices and their connectivity, firmware version and configuration. As part of the assessment, they must identify models and manufacturers of concern, such as those listed by the U.S. Government under the National Defense Authorization Act (NDAA) as presenting a high level of cyber risk. They should also document all users with knowledge of security devices and systems.

The review can pinpoint devices and systems that should be replaced. When developing a replacement program, prioritize strategies that support modernization. One effective approach is to unify physical and cybersecurity devices and software on a single, open architecture platform with centralized management tools and views.

Additionally, while physical security and IT have been approached as separate efforts historically, the risk of cyberattacks through physical security technology is driving change. The U.S. Cybersecurity and Infrastructure Security Agency recommends joining IT and physical security into a single team, so they can develop a comprehensive security program based on a common understanding of risk, responsibilities, strategies, and practices.

In the US, Federal funding may be available to help cover costs associated with replacement programs. The 2021 Investment and Jobs Act includes $1billion earmarked to help state and local governments modernize their cybersecurity.

Genetec can provide subject matter experts in public sector and security veterans to speak on this topic upon request.

--ends--

About Genetec

Genetec Inc. is a global technology company that has been transforming the physical security industry for over 25 years. Today, the company develops solutions designed to improve security, intelligence, and operations for enterprises, governments, and the communities in which we live. Its flagship product, Security Center, is an open-architecture platform that unifies IP-based video surveillance, access control, automatic license plate recognition (ALPR), communications, and analytics. Founded in 1997, and headquartered in Montreal, Canada, Genetec serves its customers via an extensive network of certified channel partners and consultants in over 159 countries. For more information about Genetec, visit: www.genetec.com

Press Contact: North America - Julie Miller, HighRez julie@highrezpr.com Tel: +1 310 259 5834