brivo®

BEST PRACTICES FOR INTEGRATING CYBERSECURITY AND PHYSICAL SECURITY

DOES YOUR PHYSICAL SECURITY PLATFORM PROTECT AGAINST CYBER THREATS?

Cybersecurity is a top-of-mind issue as the annual cost from cyber crime damage is predicted to reach $6 trillion by 2021[1]. However, your job to combat cyber risks is only getting harder as cyber criminals are more sophisticated and IT environments are more complex. One of the best cyber defenses starts at your front door with your physical security platform.

To evaluate the cybersecurity of your physical security platform, you need to ask your provider the following questions to make sure **they build products, deploy applications, and manage their internal business** in a way that keeps your company secure.

1

BUILD NETWORK SECURE PRODUCTS AND CUSTOMER PREMISE EQUIPMENT

While professional cloud-based solutions are designed to operate over public networks, systems originally designed for on-premise installation may lack precautions like strong hardware security and data secure transmission with the system server.

QUESTIONS TO ASK YOUR PROVIDER

- ☐ Does the platform reduce my "attack surface" by eliminating the need to establish open inbound ports?
- ☐ Can the platform prevent malicious attacks with bot monitoring and other security techniques for self-detection?
- ☐ Can we transition to more secure mobile credentials to prevent keycard duplication?
- ☐ For control panel authentication, is a unique digital certificate issued for each control panel during manufacturing?
- ☐ Do you offer a higher level of device communication security such as 256-bit AES encryption (same level as banks) with Transport Layer Security (TLS) 1.2 or higher?

WHAT'S THE RISK IF THIS ISN'T DONE RIGHT

Network devices can be entry points for malicious attacks when they require open inbound ports and allow unauthorized inbound communication.

1. https://cybersecurityventures.com/hackerpocalypse-cybercrime-report

2

DEPLOY AND SUPPORT APPLICATIONS

The best providers deliver 24/7 monitoring on a network with a multi-layered security model to provide redundancy, business continuity and risk management.

QUESTIONS TO ASK YOUR PROVIDER

- [ ] Is the application deployed in multiple redundant data centers to make sure my building is protected?
- [ ] Do you have active cyber defenses and a documented response plan?
- [ ] Are current applications analyzed on a regular basis to determine their vulnerability against recent cyber attacks?
- [ ] For control panel authentication, is a unique digital certificate issued for each control panel during manufacturing?
- [ ] Does the platform enable automatic software updates?

WHAT'S THE RISK IF THIS ISN'T DONE RIGHT

Without proper support and active monitoring, you could face security breaches and costly service disruptions (especially for older systems).

3

MANAGE THEIR INTERNAL OPERATIONS

For cloud providers, it's necessary to go beyond data center (AWS) provided features and accreditations and look at the certifications delivered by the application provider.

QUESTIONS TO ASK YOUR PROVIDER

- [ ] Can you provide evidence of your own audited data security controls in addition to those from your data center provider?
- [ ] Can you provide evidence of third party audits and vulnerability tests on your software, hardware and internal processes?
- [ ] Does the platform get an A grade in Qualys SSL cloud security and compliance tests?
- [ ] Do you provide a service level agreement (SLA) guarantee for platform uptime?
- [ ] Do you have strict internal personnel policies like monitoring what data and equipment your internal employees can access?

WHAT'S THE RISK IF THIS ISN'T DONE RIGHT

Providers need to limit physical access to their data center as well as key areas like backup storage and servers to protect your data.

WHY BRIVO

Brivo is the original innovator of cloud-based physical security solutions for commercial buildings. Currently serving over ten million users, Brivo offers a unified security platform including access control, mobile credentials, mobile administration, video surveillance, identity federation, visitor management, and elevator control. As a SaaS company, Brivo also offers a complete API platform service that empowers partners to build custom integrations and vertical market offerings. Our mission is to make the world a safer place by providing a subscription-based service for securing buildings using reliable, convenient, scalable, cyber-hardened technology.

For more details on cybersecurity, please read our information security white paper.

REQUEST A DEMO

brivo®
simply better security

1.833.GO.BRIVO
(1.833.462.7486)
brivo.com

You can also contact your local Brivo dealer to request additional information.