Cyber Security Checklist

For Physical Security Systems

2023

Pinnacle
SECURITY SOLUTIONS

Our mission is to provide unparalleled, high touch, and forward thinking security solutions to our clients' complex and evolving needs

rbrothers@pinnacle-security.com | 978.604.5696 | www.pinnacle-security.com

The Problem

A recent 2023 study by IBM found that ***Physical Security Compromises accounted for 8% of all cyber breaches***, and unpatched vulnerabilities accounted for another 6%. Both resulted in over $4.0 million USD in cost to the organization per incident.[1] Below are some example vulnerabilities identified over the last few years, correlated with the sample architecture diagram below. ***These examples do not include potential vulnerabilities related to user privileges, access privileges, end-of-support devices, or Windows OS and SQL databases.***

1. Axis cameras riddled with vulnerabilities enabling “full control”
2. How we copied key fobs and found vulnerabilities in keycards
3. Next-gen OSDP was supposed to make it harder to break in to secure facilities. It failed.
4. Researchers disclose critical flaws in industrial access controllers...
5. Critical flaws in Cisco switches could allow remote attacks
6. Vulnerabilities expose Exacq video systems to remote attacks
7. Security vulnerability affecting Security Center
8. Incorrect access control in AMAG Symmetry door controllers

Basic Access Control and Video Management Architecture

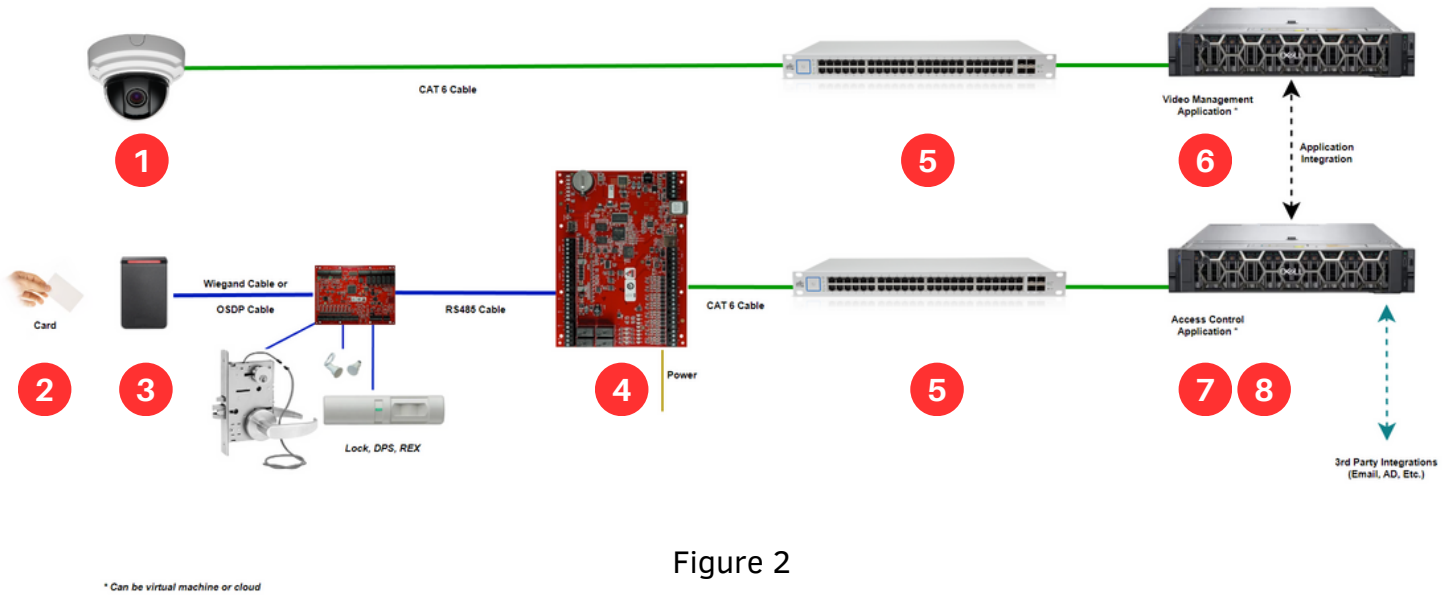

Figure 2

The Checklist

FIELD DEVICES

- [ ] Are your credentials 13.56 MHz with secure encryption?
- [ ] Are you utilizing OSDP cabling and encryption for card reader secure communication to controllers?
- [ ] Has security panel firmware been updated in the last 12 months?
- [ ] Has camera firmware been updated in the last 12 months?
- [ ] Is hardware systematically tested on a monthly basis (to include door hardware)?
- [ ] Are end-of-support or manufacturing devices replaced or scheduled to be replaced regularly?
- [ ] Are devices NDAA compliant?

PRIVILEGES

- [ ] Are default passwords disabled? Are service or technician passwords unique (many are repeated across clients)?
- [ ] Are access privileges automated or managed by group membership?
- [ ] Are user privileges restricted and managed by group membership?
- [ ] Are access privileges audited regularly?

UPDATES

- [ ] Are Windows or OS patches applied monthly?
- [ ] Are application updates applied annually for access control and video management systems?

STANDARDS

- [ ] Does your organization have standards and/or guidelines for security system design and approved parts list?
- [ ] Has your organization implemented cyber-hardening guides?

MONITORING

- [ ] Does your organization monitor alarms and track anomalies?
- [ ] Does your organization utilize metrics and key performance indicators to measure system operations and health?

"[The Pinnacle Team] consistently showcased knowledge, honesty, and an exceptional work ethic. [The Team] demonstrated expertise and critical-thinking skills by cleverly finding solutions to problems"

-Large University

Additional Information

According to the 2023 World Security Report[2]

- 35% of organizations lack the internal expertise to implement and manage security technology
- 40% of organizations cite a lack of funding to maintain their security systems as a barrier
- 90% of organizations stated that technology improves the overall effectiveness of security operations

We are here to help bridge the information gap!

References

1. *International Business Machines Corporation. Cost of a Data Breach 2023. IBM, 2023. [Online]. Available at: https://www.ibm.com/reports/data-breach [Accessed 2023-10-11].*
2. *Allied Universal. World Security Report 2023. [Online]. Available at: https://www.aus.com/world-security-report [Accessed 2023-08-04].*

Pinnacle Security Solutions

Your Independent Guide to Security Excellence

Phone Number

978.604.5696

Email Address

RBrothers@Pinnacle-Security.com

Website Address

www.Pinnacle-Security.com

Contact us now for a free initial consultation!