SecureLink®

The Hall of Unlocked Doors

How one opening can lead to many in an organization's system

Finding The Right Door

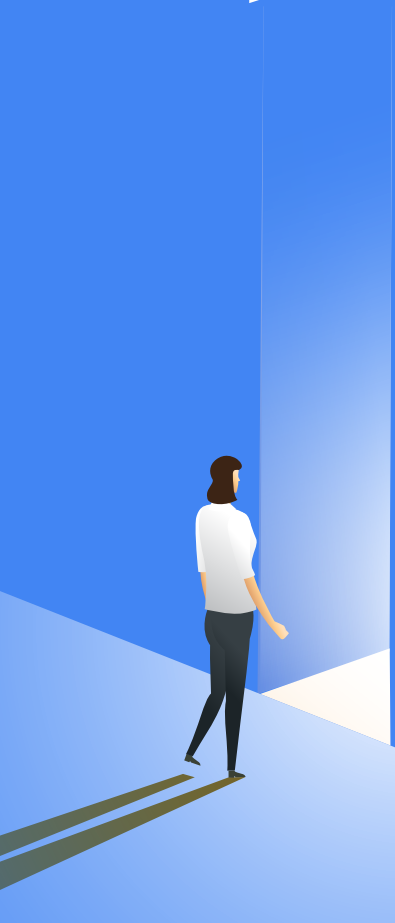
To initiate a hack, a bad actor needs to find the right door into an organization's cyber architecture. Every door should (in theory) be locked, so it's a matter of picking the lock (like finding a compromised password on the darkweb) or knocking and hoping a user lets them in (as is often the case in phishing scams).

One Door Unlocks Many

Most organizations are still employing a "castle-and-moat" style of cyber security, so once that bad actor picks the lock on the first door, they're greeted with minimal security guards and a hall of potentially unlocked doors that lead to anywhere and everywhere in the system, including sensitive data, OT, and more. Every internal door is swinging open, waiting for a bad actor to walk through.

A Full System Is Breached

The consequences of these kinds of breaches are deep and vast. It could include: holding OT systems ransom for millions to stealing sensitive data to using an organization as a tunnel into another organization through those third-party points of access.



COLONIAL PIPELINE HACK:

The Colonial Pipeline ransomware attack is the perfect example of how by just picking the lock of one door, a hacker was able to walk through many.

- A hacker was able to find, on the darkweb, a password to a VPN login for an employee that was never properly deprovisioned after access was no longer needed. This VPN lacked multi-factor authentication or other cybersecurity measures. It was a single sign-on.
- Through this VPN, the hacker was able to move laterally through unlocked doors in the system, and was able to access control technology and set up a ransomware attack.
- Because every metaphorical door in Colonial's system was unlocked, the only response was to shut everything down. This resulted in reputational damage, gas shortages across the Southeast United States, and a ransom payment of $4.4 million.

Better understand your organization's vulnerabilities and how to protect critical access points with our Critical Access Management ebook.