How an Attacker Bypasses Network, Software and Physical Controls

Conexxus Data Security Webinar: What you missed

September 8, 2020 • Published by Jeff Gibson (https://www.controlscan.com/author/jeff-gibson/)

These past few months have underscored the need for all of us to maintain open and consistent communication with one another. Without the opportunity to interface with our colleagues and peers in a daily office setting or face-to-face meeting, the ability to share industry-related news quickly and easily is imperative to ensure business proceeds as … well … *the new* normal.

As we refine our remote work arrangements, though, our arsenal of communication devices —and our digital footprint—grows. Smartphones, tablets, e-readers, laptops, desktops (and don't forget game consoles!) are everywhere.

Unfortunately, all these communication tools create additional IT vulnerabilities and make our businesses a more prominent target for cyber attackers to exploit. It goes without saying that defending against such attacks is critical for protecting a business's assets as well as the integrity of its network architecture.

So how does an attacker bypass network, software and physical controls in today's extended workplace environment? I was honored to co-present on this topic at a recent Conexxus data security webinar (https://youtu.be/3VRuct3iyhs), and I'd like to share some of my primary points with you now.

Common Attacker Bypasses

As corporate workforces disperse remotely, their networks include a proliferation of scattered endpoints, making the oversight of electronic data and their physical infrastructure fraught with challenges.

Meanwhile, cyber attacks have evolved (https://www.controlscan.com/blog/cybercriminals-taking-advantage-coronavirus-fears/) from the blatantly spam emails seeking emergency relief for stranded travelers. Today, an attacker employs advanced tactics to target a digital buffet of ripe attack points: desktop/servers, hosted and third-party applications, payment devices, infrastructure access, guest/employee access, IoT and BYO device, emails and text messages, to name just a few.

Businesses today must address a multitude of risks simultaneously and continuously. Let's talk about just a few common attacker bypasses.

Third-Party Applications

Nearly every company today relies on third-party applications like Dropbox or Office 365 or QuickBooks, etc. (the practice extends to personal use, too, where Zoom has become the de facto communication tool for remote learning).

While the third-party offerings make running your business easier (streamlines processes, reduces capital expenditures), they come at a cost: increased data security risk. That is, if the third-party supplier doesn't maintain a strong security posture and is compromised, the impact has a good chance of trickling down to your business.

I recommend asking any prospective service provider (https://www.controlscan.com/data-security-vendor-management/) whether they have had a Level 1 PCI assessment and an AoC dated with the last 12 months. If not, this is a red flag and you should consider other options.

Email, Text and Voicemail

Security awareness must extend to all messaging platforms, which have come under "-ishing" attacks—phishing (email), vishing (voicemail), and swishing (text). Education is key to preventing unwitting access to your company's messages, and thereby its network.

Best practices include teaching password hygiene (still entering John123? Ugh), establishing protocols for incident reporting and response, and implementing robust malware solutions (hint: if yours is a legacy antivirus that requires a 10-minute download of updates to offer malware *detection*, look elsewhere; we favor an approach that focuses on detection, prevention and response (https://www.controlscan.com/security/endpoint-security/)).

Guest and Employee Access

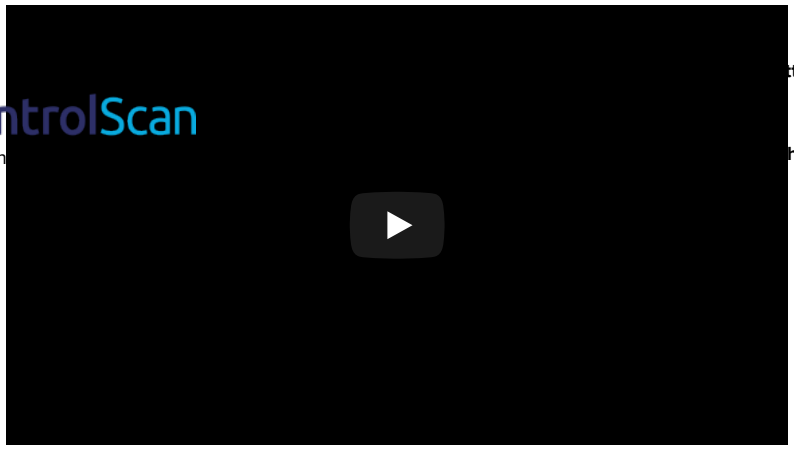
Still allowing vendors and their well-traveled laptop to tap into your organization's primary Wi-Fi when they're on a sales call? If so, understand that vulnerabilities in that person's computer, once they gain access to your network, provide backdoor access for a cyber attack. And those weaknesses carry over to "Bring Your Own Device" policies among employees (rather than company-distributed equipment), where an unstructured approach to security helps grow your digital footprint—and vulnerabilities—yet again.

Moving Ahead with Cybersecurity

There are many other primary risks, and rest assured, the list is growing. Vigilance here is key; an ongoing pursuit to defend your property and assets against intruders and preserve your network.

But one final thought here: this is a top-down requirement, not an IT concern. The best way to protect is to educate, implement and enforce a strong security program across your entire organization. Without it, you simply create additional potential for attacker bypasses.

View the Conexxus webinar, "How an Attacker Bypasses Network, Software and Physical Controls" below:



of-sale/) Privacy (https://www.controlscan.com/tag/privacy/) Ransomware (https://www.controlscan.com/tag Risk Management (https://www.controlscan.com management/) Security Assessments (https://www.controlscan.co assessments/) Security Awareness (https://www.controlsc awareness/) SIEM (https://www.controlscan.com/tag/siem/) Social Engineering (https://www.controlscan.co engineering/) Vulnerability Management (https://www.controlsca management/) Website Security (https://www.controlscan.com/t security/) Wireless Security (https://www.controlscan.com/tag/wireless-security/)

(https://www.linkedin.com/company/controlscan) (https://twitter.com/ControlScan) (https://www.youtube.com/user/ControlScan)