SEVEN NETWORK ACCESS SECURITY RISKS

AND HOW THEY CAN LEAD TO A DATA BREACH

RUCKUS®
COMMSCOPE

INTRODUCTION

IT teams struggle with how to prioritize various forms of protection when it comes to network and data security. The IT security taxonomy is vast. What attack surfaces are the most likely to lead to a data breach? Often, it's the ones that you aren't thinking about that leave your IT environment most vulnerable—the areas that don't garner headlines and aren't necessarily top of mind. Attackers seek out weaknesses in places where you don't see them coming.

Network access security is one area that IT organizations may underestimate as an attack surface. Failure to properly secure network access, especially for BYOD and guest users, is an area that's ripe for attack in many organizations. It can leave you open to a breach that would compromise your data security and user privacy. This e-book will help you to understand the risks.

How Poor Network Access Security Can Lead to Data Compromise

DATA BREACH RISK 1

Prying eyes can intercept unencrypted data traffic

Attackers can intercept unencrypted wireless data traffic using commercially available network analysis tools. While most websites are encrypted these days, they often do not encrypt every component on the page. Users have no visibility into what elements are encrypted, and they are too busy interacting with the page to even think about it. Mobile applications often do not encrypt their data traffic—and the fact that encryption imposes some backend system overhead gives developers an incentive not to use encryption. Secure access requires strong encryption for data traveling over the air between wireless access points and devices. Two security protocols for this purpose are WPA2 and WPA3.

DATA BREACH RISK 2

Unsecured devices can let malware enter your IT environment

Organizations in a wide variety of industries have adopted BYOD programs because they are great for employee productivity. But unmanaged devices can bring greater risk if they don't employ proper security measures. They may be more likely to carry malware, which can compromise sensitive data. If you don't make sure that BYOD devices have appropriate safeguards in place before they connect, you increase the risk that an infected device joins the network. An up-front security posture check can mitigate this risk as part of a layered malware defense. A posture check can ensure that employee laptops have up-to-date anti-malware software installed. It can also make sure that other security measures are in place—for example, you can require that users enable desktop firewalls on their laptop and enable a PIN code on mobile devices.

DATA BREACH RISK 3

Unapproved users might connect to the network

Depending upon your method for BYOD and guest network onboarding, unapproved users can connect to your network. If everyone, or even groups of users, shares the same Wi-Fi password, that means they can give that key to their friends, their family or anyone at all. Many organizations have it written on a white board, or sticky note posted on the wall. When you can't control who gets access, you are leaving the door wide open to a data breach. Network access security is as much about who doesn't get access as about who does. The best approach is to authenticate users and devices individually, so that only approved users can connect.

DATA BREACH RISK 4

Users can get broader access than appropriate

Sound data governance requires that you provide access to your organization’s sensitive data on a need-to-know basis. Without a way to authorize users for the right level of network access, you are leaving the door wide open for misuse of that data—whether intentional or accidental. To prevent a data breach, best practices require limiting access based upon the user’s role in the organization. You may also want to limit access based upon the type of device. Network access policies provide a mechanism to do both. Some organizations try to do this with multiple SSIDs, but there is no way to ensure that users and devices connect to the right SSID. Besides, SSID proliferation clutters your environment and may provide cover for other kinds of attacks.

DATA BREACH RISK 5

Attackers may trick users with rogue access points

A rogue access point is any AP that is not approved and managed by IT. Not every rogue is malicious. An employee may set one up to extend coverage—an action that is innocently misguided. Some rogues are malicious, and they may even trick users into divulging confidential information. A Wi-Fi phishing attack can compromise wireless credentials, logins for your single sign-on system or other applications—even users' personal digital identities. Attackers often perpetrate data breaches using valid login credentials, and this is one way they can obtain them. Or imagine the damage they could inflict on your organization's reputation if they gained access to an executive's personal email or social media account.

DATA BREACH RISK 6

Inability to revoke access can leave you vulnerable

Users should only be able to access your network for as long as their relationship to the organization merits it. If an employee leaves the organization, you don’t want them accessing internal servers from the parking lot over a Wi-Fi connection. Strong network security requires that you be able to reach in and revoke access for specific users without affecting others. It’s also a good idea to be able to revoke access only for certain devices. For example, if there is a critical security alert for a specific operating platform, you might need to cut off access for certain devices until users remediate them. But you wouldn’t want to disrupt users from accessing the network on other platforms that are unaffected by the security alert. Without the ability to revoke access in a granular fashion, your network is more vulnerable.

DATA BREACH RISK 7

Lack of visibility can expose your data assets

Proper IT security controls mean having maximum visibility over who and what devices connect to your wired and wireless network. Suppose someone used the connectivity that you provided to perpetrate a phishing attack, or to plant malware in your environment. IT teams can't put a stop to usage violations that might breach data security if they can't associate a user with a device. You can't control what you can't see—and your level of control for BYOD devices is already less than it would be for IT-owned devices. Best practices for secure network access require both visibility into what devices are on the network, and what user is associated with every device.

What Can IT Teams Do to Plug These Security Holes?

A layered defense against data compromise is essential, and network access is one attack surface that is easy to underestimate. Security measures that are built into your network infrastructure—like wireless intrusion detection and prevention—offer important protections. But built-it methods for onboarding and authentication fail to address the full range of network access security threats. A purpose-built system for secure network onboarding addresses the security shortcomings of the default methods that you may be using today. Digital certificates as the basis for network authentication ensure that every connection is secure for BYOD users, and server certificate validation provides additional protection against rogues.

Learn more at www.commscope.com/secureaccess

www.ruckusnetworks.com

Visit our website or contact your local RUCKUS representative for more information.

RUCKUS®
COMMSCOPE