5 Compelling Reasons to Ditch Wi-Fi Pre-Shared Keys (PSKs) Now

https://www.linkedin.com/pulse/5-compelling-reasons-ditch-wi-fi-pre-shared-keys-psks-de-oliveira-rob2e/?trackingId=FMTeUOGISR680DUCwMDmsw%3D%3D

For many years, we have advised our clients on the critical importance of moving away from using Wi-Fi pre-shared keys (PSKs) on their corporate networks. With the increasing awareness of data sensitivity, it is essential to take network security and data protection more seriously.

The growing understanding of data sensitivity, driven by PCI compliance, GDPR regulations, and several high-profile security breaches, has made securing networks and the data they contain the top priority for companies. Here are five reasons why relying on a simple Wi-Fi pre-shared key for network security is no longer acceptable.

1. Wi-Fi Password Keys Are Rarely Updated □□

The inconvenience of regularly updating pre-shared keys on all client devices means they are seldom changed. This increases the likelihood of them being compromised over time. Whenever an employee leaves, a laptop or device is lost or stolen, or a significant period passes, the PSK should be updated. Delaying this increases the risk of a security breach.

2. Lost or Stolen Devices Can Expose Your Wi-Fi Password □□□

With easily accessible tools available online, extracting a Wi-Fi PSK from a device can be done quickly. Combined with the fact that Wi-Fi passwords are infrequently changed, this can lead to unauthorized network access. Ideally, you should change your Wi-Fi password whenever a device is lost, but this is rarely practiced.

3. Wi-Fi Password Keys Can Be Easily Guessed □□

Due to the complexity involved in managing and sharing PSKs, administrators often opt for simple and memorable passwords. This approach significantly weakens security, as hackers can employ brute force attacks to guess these keys and gain network access.

4. Wi-Fi Password Keys Can Be Easily Shared □□

Employees remain a significant threat to network security, often inadvertently sharing network keys. Features like Apple's iOS 17 Wi-Fi password sharing enable easy distribution of network passwords with a few clicks. IT teams may also display Wi-Fi passwords on noticeboards to reduce connectivity issues, further compromising security.

5. Perceived Complexity of Alternatives is a Myth □□

The belief that alternatives to PSKs are overly complicated is outdated. While 802.1X implementation involves multiple components (e.g., Network Policy Server, Certificate Server), modern Wi-Fi onboarding security solutions have simplified the process.

The transition from pre-shared passwords has never been easier with solutions like Ruckus Cloudpath or Cisco Spaces as some examples. These advanced Wi-Fi security and onboarding solutions support any device or OS, providing certificate-based authentication in an easy-to-use package.

Investing in advanced security measures is not just a recommendation; it's a necessity in today's environment. Strengthen your network security by moving away from outdated Wi-Fi pre-shared keys to more robust and manageable solutions. □□□□

Best Practices for Secure Wi-Fi Onboarding and Management

To further enhance your network security, here are some best practices to consider:

1. Implement Certificate-Based Authentication

Use certificate-based authentication for devices to ensure that only authorized devices can access your network. Solutions like Ruckus Cloudpath and SecureW2 offer robust options for managing digital certificates.

2. Regularly Update Security Protocols

Ensure that your network security protocols, such as WPA3, are up-to-date. This adds an extra layer of protection against potential vulnerabilities.

3. Conduct Regular Security Audits

Regularly audit your network security to identify and address potential weaknesses. This includes reviewing access logs, conducting penetration testing, and ensuring compliance with security standards like PCI DSS and GDPR.

4. Educate Employees on Security Practices

Provide regular training to employees on the importance of network security and best practices for protecting sensitive data. This includes avoiding the sharing of Wi-Fi passwords and recognizing phishing attempts.

5. Utilize Network Access Control (NAC)

Implement NAC solutions to manage and control device access to your network. This ensures that only compliant devices can connect, reducing the risk of unauthorized access.

6. Segment Your Network

Use network segmentation to isolate sensitive data and critical systems. This limits the potential impact of a security breach by containing it within a specific segment of your network.

By following these best practices, you can significantly enhance your network security, ensuring that your organization's data remains protected and your network remains resilient against potential threats.

#SecurityBestPractices #NetworkSecurity #CyberSecurity WiFiSecurity #SecureWiFi #Infosec #SecurityBestPractices

---

Revision #2
Created 12 July 2024 05:06:24 by Jarryd
Updated 4 October 2024 05:04:47 by Jarryd