What can I do to protect my wireless network?

Whether or not you are a SonicWall wireless network security user, we do recommend that you take immediate action to minimize the risk presented by these vulnerabilities. We advise the following:

- Patch all of your WiFi clients, whether Windows, Linux, Android, iOS or Mac OS based, with the latest KRACK updates from your client vendors. The attack is launched by compromising the wireless device, not the wireless router, so that is the most important area to focus on when you go about patching.
- If you are not a SonicWall wireless customer, check with your vendor to determine if you need to patch your wireless access points and/or routers. Ideally, your WiFi solution would be centrally managed allowing you to provide updates and patches in a timely fashion without crippling IT resources. Again, if you are a SonicWall wireless customer no updates to the access points are needed.
- Add an additional layer of security by using VPN technology to encrypt all network traffic between your wireless devices and your firewall. For SonicWall customers, we recommend the following:
    - For SSL encryption on mobile devices, use the SonicWall Mobile Connect client, which is available on the Apple App Store, Google Play, Windows Phone Store or Chrome Web Store.
    - For IPsec encryption, use the SonicWall Global VPN Client.
- Advise your users to transmit sensitive data only on TLS/SSL-encrypted web pages. Look for the green lock symbol in the address bar along with *https* in the URL.
- The new SonicWall SonicWave series includes a dedicated third radio for scanning. For SonicWave wireless users, we recommend that you turn on the wireless intrusion detection feature that allows you to block traffic from rogue access points (specifically in this case an evil twin). This will ensure that the third radio is continually scanning for these types of attacks in real-time.
- Be on the lookout for unusual activity inside or outside your facility. In order to launch an attack using these vulnerabilities, an attacker must be physically located within Wi-Fi range of both the access point and the wireless client that is attempting to connect to the network. That means the attacker must be in or near your building, which makes it a bit more difficult to leverage than other Internet-only attacks.

- One other note: there is no need to change Wi-Fi passwords as the KRACKs do not require the Wi-Fi password to be successful.

SonicWall believes that IT must be able to provide secure, high-speed access for the organization across both the wired and the wireless network, especially as Wi-Fi becomes more of a necessity and less of a luxury. However, cyber criminals are racing to leverage wireless to initiate advanced attacks.

SonicWall can help you extend breach prevention to your wireless network. SonicWall's wireless network security solution provides deep packet inspection for both unencrypted and TLS/SSL-encrypted traffic along with a cloud-based, multi-engine Capture sandbox and a complete lineup of centrally managed SonicWave 802.11ac Wave 2 wireless access points.

For further assistance, please contact your Account Manager on 0800 023 2696 of email us – info@newcmi.com

THE SECURITY TEAM