ARTICLE FROM Forbes

Current Geopolitics Are Raising The Need For New Cybersecurity Measures

Contributor: Will Townsend

It is tragic to witness what is happening in eastern Europe. The conflict is near my heart, given that a good friend recently fled Kyiv with his wife, but it also raises broader public awareness of nation-state cyber-attacks. These virtual assaults are nothing new. A report published by IBM Security X-Force (a very Marvel comics-sounding team!) noted a staggering 3,000 percent increase in IoT malware activity from mid-2019 to the end of 2020, just as the Covid-19 pandemic was gaining momentum and companies shifted to remote work.

Flash forward to the present day. The U.S. government is warning enterprises of potential Russian cyberattacks as the mass exodus of companies such as Starbucks and McDonald's continues amid economic sanctions. Indeed, many of these iconic American companies are in the crosshairs of Russian saboteurs as retribution for the exits. However, a more significant concern is the possible attack and subsequent impact on critical infrastructure. From my perspective, transportation, energy, manufacturing, and telecommunications are at the highest risk, and the ramifications would be incalculable on our home front. These sectors broadly deploy IoT headless devices and sensors, which can be easily hacked, complicating the situation. Thus, security operations teams will need to consider deploying new security measures to thwart the onslaught of attacks.

> "From my perspective, companies such as Airgap are rising to the challenge with new architectures and tools to provide a layered approach to thwarting an ever-growing cybersecurity threat."

The 5G and Open RAN effect

The deployment of super-fast 5G networks will also impact an ever-growing threat surface that IoT has extended. The new cellular standard can inherently support a significant number of more connected devices relative to 4G LTE and facilitate industrial IoT adoption for manufacturing automation. However, despite improvements in security in the 3GPP 5G New Radio standard, continued interest in Open Radio Access Network (Open RAN) infrastructure in public and private 5G network deployments could pose incremental security risks. Open RAN promises to reduce capital and operational expense levels and improve deployment agility. However, its disaggregated nature and shallow focus on security, as evidenced by a lack of security working groups among the various Open RAN alliances, raise concerns.

Airgap Networks

What should organizations across multiple vertical sectors consider given the escalation in cyber-attacks? Many security solutions available, but what could be beneficial is an additional layer of protection for managing networked devices and application access. Additionally, tools that can quickly improve visibility and neutralize ransomware attacks are powerful. I have been following startup Airgap Networks for some time now, and its recent round of Series A funding of nearly $14M reported in February may serve as a testament to what it can provide in the cyber defense of the world. I have also written about Airgap in the past, and if you are interested, you can find that article here.

Network segmentation is designed to ringfence every endpoint, implement zero-trust provisions across LAN, data center, and cloud, and employ autonomous policy and artificial intelligence to facilitate policy decisions. Airgap's ability to do all the above without device agents is compelling. It doesn't modify existing networking infrastructure and can work with headless devices found in many Operational Technology (OT) environments. Airgap is also trailblazing the Secure Asset Access (SAA) category. SAA aims to employ zero trust principles by enforcing integrated single sign-on (SSO) before granting remote access to any private application.

I like Airgap's approach with a flexible platform deployed on existing networking infrastructure as a virtual appliance that doesn't prescribe a particular cloud on-ramp or require agents on devices. The result is a solution that can function across traditional carpeted IT and OT environments and is manageable from a single pane of glass, providing visibility, ease of management, and potentially lower operational expense for NetOps and SecOps teams. If that isn't enough, Airgap claims that its Ransomware Kill Switch is the industry's only software "easy button" that can stop a ransomware attack in its tracks. In conversations with the company's executive leadership team, I learned that the solution's strength lies in its five filed patents, significant refinement in the form of extensive customer feedback, and thousands of development hours invested in its development.

Wrapping up

The growth of remote work born out of the pandemic provides bad actors ample opportunity to test the vulnerabilities of networking infrastructure. The current geopolitical climate has only fanned cyberattack flames further and raised public and corporate concern. Companies across multiple industries will embrace IoT and private 5G networks for the resulting benefit of accelerating digital transformation, but it will place additional pressure on security postures. From my perspective, companies such as Airgap are rising to the challenge with new architectures and tools to provide a layered approach to thwarting an ever-growing cybersecurity threat.

About Airgap Networks

Airgap provides an agentless Anti-Ransomware platform to stop the spread of malware in the enterprise network. Our industry's first Ransomware Kill Switch™ locks down your most critical network assets at the first indication of compromise with complete control and policy enforcement over the device-to-device and device-to-application communication.

AIRGAP™

airgap.io