M+E JOURNAL

It's Showtime!

Innovation explodes across every workflow as technology emerges from the pandemic.

Where are you in this accelerated evolution?

DIVERSITY & INCLUSION
In the office, behind the camera, and on the screen, diversity is crucial

SECURITY
Remote productions create new security concerns, with assets under siege

SMART CONTENT
Artificial intelligence and machine learning are being applied in new, exciting ways

NEW WORKFLOWS
The cloud is delivering on its promise, powering the future of productions

21.01

CYBER WARFARE: ADDRESSING A VERY REAL THREAT TO THE M&E INDUSTRY

It's critical to leverage every tool available to combat today's highly motivated cyber criminals.

By Gary Davis, Chief Marketing Officer, INTRUSION

ABSTRACT: Recent cyberattacks have proven we're no longer fighting just hackers: nation states have waged cyber warfare on our economy, and no industry is safe. Cybercriminals can live in the networks of media and entertainment companies for months, learning their most valuable assets and ways to disrupt business. We need a new approach to cybersecurity.

It's all over the news. Massive cyberattacks disrupting critical businesses, systems and government organizations, and it seems there's a new one every day.

Even some of the top cybersecurity companies are being brought down or severely disrupted by substantial, harmful attacks to their systems. This is a clear signal that our approach to cybersecurity has failed.

CYBERCRIME HAS EVOLVED. THIS IS CYBERWAR.

What does this mean? Cyber warfare is more far-reaching than cybercrime and rightly classified as a war because it often includes the full resources of nation-states whose goal is to slow down an adversary (in this case U.S. businesses), steal secrets or inflict pain. These are foreign aggressors who have spent decades trying to break down and dominate their enemies and want to capitalize on whatever they can, whether that is new technologies, a crisis or vulnerabilities. They are, in fact, leading PhDs and computer scientists employed by their governments with well-funded budgets that exceed the military spending of some third-world countries.

It's time for all U.S. organizations, small and large, to rethink our approach to cybersecurity in order to address this cyber warfare.

For media and entertainment companies, this means bolstering the ways in which we protect critical, confidential assets and content. The opportunities for cybercriminals to disrupt businesses within the industry are vast. Criminals are not just breaking in and stealing whatever they can find as quickly as possible. They will breach a network and live there for months, years even, looking for the most valuable information to steal and the best ways to cause damage.

What could a cybercriminal access on your network given the time to search for it? One of the most common attacks media and entertainment companies face is ransomware, where adversaries identify your most valuable assets and hold them hostage until you pay a ransom. Several large studios and streaming companies have fallen victim to this type of attack where episodes, scripts, and more were stolen, with a threat to have them leaked until the organization paid a fee to have their assets returned. And for sports organizations, criminals could target sensitive documents, including trading and recruiting plans.

These nation-states can also cause massive disruption with the information and assets they access. For example, an attack on the 2018 Winter Olympics in South Korea, disrupted the opening ceremonies. A soccer team in the UK was the victim of an attack where the criminals shut down the turnstiles in the team's stadium, preventing fans from entering or exiting. All of these issues can cost organizations money, time, and reputation.

So, what is the best way for media and entertainment organizations to protect themselves?

For too long, the cybersecurity industry has focused on keeping adversaries out of networks with firewalls. Unfortunately, it's no longer effective to try to keep criminals out: they find their way in faster than we can develop new locks for the door. Once inside, attackers have a lot of freedom to talk to other machines on a network, look around for data, establish improved credentials, and download critical information with little-to-no real-time oversight.

Firewalls are important, but it's important to have additional defenses to protect critical assets. Appliances that monitor network traffic and alert to threats are important, as well as solutions that protect an organization's computers that are not directly connected to the network, such as a VPN.

FIREWALLS are important, but it's important to have additional defenses to protect critical assets.

But even these layered approaches have resulted in serious breaches. We have to do more. It's time to rethink the ways in which we defend our critical assets. Here's how:

Assumption of infection: It's important that we assume that cybercriminals have already found their way into our networks. Because firewalls are not foolproof, we have to act as if they are already inside our network, searching for our most valuable assets.

Monitoring outgoing traffic: Once these criminals are in a network, it's impossible for them to do any damage unless they can "call home," or send information back to their servers. Utilizing a tool that is monitoring outgoing traffic and has the ability to not only identify it as malicious — either based on it being a known threat, or utilizing artificial intelligence to identify it as malicious based on its activity — but also to kill that threat in real time. Stopping your assets from ever leaving your network is the only way to keep them completely from being compromised or used in a ransomware attack.

Reduce false positives: Many solutions have high rates of false positives, meaning they identify a packet of good data as a threat. This not only disrupts an organization's operations — keeping them from getting work done — but also sends network managers on a hunt that takes up time and resources.

It's critical that we leverage everything possible to combat these highly motivated cyber criminals. The next big breach we see in the news could easily be a media company, sports league or team. Before that happens, let's shift our thinking around cybersecurity and start protecting our valuable assets and networks from the inside out. ⊞

Gary Davis *serves as INTRUSION's chief marketing officer. He brings more than 20 years of executive marketing experience and a proven track record of driving profitable growth. His extensive experience spans both business-to-business (B2B) and business-to-consumer (B2C) marketing for technology companies.* *info@intrusion.com* *@INTRUSIONShield*

INTRUSION™

Protect everything. Trust nothing.

INTRUSION *Shield* protects your network from Zero-Day Attacks

Shield looks at all traffic – inbound *and* outbound – to identify malicious communications and kills them before they can cause harm, keeping your network safe.

Largest IP source database cloud

Shield uses the ***TraceCop***™ cloud containing the full history and reputation of every domain, IP and every host to ensure your company is protected from every threat.

Real-time AI kills all malicious traffic

The AI deep learning algorithm applied to the knowledge of ***TraceCop*** as well as the logic of our ***Savant***™ networking monitoring solution makes ***Shield*** the most advanced cyber attack prevention solution available.

Unrivaled accuracy

At 99.999% accuracy, rest assured that ***Shield*** is only killing bad traffic and not slowing down good traffic.

Learn more at intrusion.com