LOGPOINT

May 16, 2022 09:57 CEST

Cybersecurity protection is a corporate social responsibility – especially during times of war

Failing to protect your organization against cyberattacks does not only endanger your enterprise – it also puts your business partners and broader society at risk, especially during times of war like the ongoing war in Europe

By Jesper Zerlang, CEO, Logpoint

Through cyberspace, all organizations are potentially part of the war. In an effort to prevent detrimental cyberattacks, US president Biden recently

signed legislation requiring critical infrastructure entities to report any cyberattacks within a specific timeframe, and the same goes for the EU which has had similar legislation in place. However, organizations in other industries are not immune and should be preparing for similar threats. It's no longer a question of *if* a business will be targeted but *when*.

Critical infrastructure or not. Intentionally or not. Voluntarily or not. State-operated cybercriminals, state-sponsored hackers, and cyber groups, publicly announcing support for Russia, are already preparing to deploy cyberattacks to wreak havoc and disrupt vital services, government functions, and communication to the public.

Organizations have a corporate social responsibility (CSR) to implement strong cybersecurity defenses and prepare for a scenario in which Russia deploys cyberattacks on an unprecedented scale. There are many ways an organization could become hostage in a global cyberwar.

The threats

A favored method of state-sponsored threat actors is the supply chain attack in which the attackers target a trusted partner or a third-party to deploy their attacks. For example, Toyota recently had to shut down 14 factories and 28 production lines for an entire day because of an attack through a sub-supplier.

In this threat landscape, organizations risk becoming the gateway to supply chain attacks on critical infrastructure organizations, like electricity, financial services or hospitals.

Another widely used vector is DDoS attacks aimed at disrupting services by overloading servers and infrastructure, which we have seen in both Ukraine and Russia. Attackers need so-called botnets to deploy these attacks and hijack unsecured devices, such as IoT devices, to amass the traffic needed to cripple vital services.

Imagine Russian state-sponsored actors taking control of your network and infiltrating key components of your product or service – making you unknowingly appear as the aggressor against your own business partners.

Ransomware attacks have drawn headlines throughout the last years, with high-profile attacks on Colonial Pipeline, JBS, and Kesaya. CNA Financial reportedly paid 40 million dollars to regain access to files and get their operations back up. The ransomware threat has proven widespread and destructive. And last week the US indicted Russian nationals that are allegedly part of sophisticated attacks on critical infrastructure.

Considering cybersecurity protection as CSR 24/7

Several ransomware groups have declared allegiance to Russia. Falling victim to a ransomware attack by these groups could cause organizations to lose access to critical data forever or pay the ransom and potentially contribute financially to the continued hybrid war.

The list of ways to neglect CSR through poor cybersecurity goes on. And it's important to note that the responsibility is not just relevant in times of war. Cybersecurity has always been a corporate social responsibility. But it has never been as evident as now.

At all times, organizations without proper cybersecurity are assuming a significant risk on their customers, employees, partners and surroundings behalf because of the ever-present threat of supply chain attacks, data theft, ransomware attacks, DDoS attacks with real human and societal impact.

The ransomware attack on the Colonial Pipeline, leaving Americans without gas for weeks; the supply chain attack on Kesaya forcing COOP to close supermarkets in Sweden; the cyber intrusion that enabled cybercriminals to change the sodium hydroxide levels in the water supply to dangerous levels in Florida – all attacks occurred because guards were down.

Now is the time to act if you haven't yet put cybersecurity at the top of your corporate agenda. It's crucial for businesses to be able to mount a robust cybersecurity posture capable of defending against known and unknown cyber threats.

Taking initiative

During the cybersecurity labor shortage, hiring enough competent employees can be difficult. Businesses can instead look to AI and automated solutions or

partner up with a Managed Security Service Provider that provides 24/7 cybersecurity with sufficient capabilities to detect and respond to cyber threats.

Further, businesses must do away with the mindset that cyberattacks won't happen to them and stop assuming that securing only the outer perimeter keeps them safe. It just takes a single cybercriminal to succeed once in slipping through the cracks and gain access to your IT environment and make your organization part of a bigger cyberattack or jeopardize the operation of your company.

The current war has sparked Western organizations to pledge their support to Ukraine, with many businesses halting engagements with Russia, in the form of sanctions, corporate responsibility standards or to manage their reputation. However, overlooking how cybersecurity acts as a form of CSR puts organizations, their clients and their employees at risk of becoming tools to aid Russia in their cyber warfare, contradicting their original good intentions to denounce Russia.

About Logpoint

Logpoint is the creator of a reliable, innovative cybersecurity operations platform — empowering organizations worldwide to thrive in a world of evolving threats. By combining sophisticated technology and a profound understanding of customer challenges, LogPoint bolsters security teams' capabilities while helping them combat current and future threats. Logpoint offers SIEM, UEBA, SOAR and BCS technologies converged into a complete platform that efficiently detects threats, minimizes false positives, autonomously prioritizes risks, responds to incidents, and much more. Headquartered in Copenhagen, Denmark, with offices around the world, Logpoint is a multinational, multicultural, and inclusive company. For more information, visit http://www.logpoint.com

Contacts

Maimouna Corr Fonsbøl
Press Contact
Head of PR
PR & Communications
mcf@logpoint.com
+45 25 66 82 98