WHAT YOU NEED TO KNOW NOW ABOUT CYBERSECURITY IN EVENTS

SMARTSOURCE

CYBERSECURITY IN EVENTS

Cybersecurity has been an issue for companies, including event organizers, throughout the pandemic, especially with a remote workforce still in place. However, the Russia-Ukraine conflict may eclipse any COVID-related cyberthreat scenario by orders of magnitude, experts say. Here's an updated review of the risks and what organizations must do to help protect their event assets from attacks.

An article on the Harvard Business Review website suggests that the war with Ukraine has been serving as a live testing ground for Russia's next generation of cyber weapons. In 2015, Russian hackers knocked out power to 230,000 Ukrainians, adding government agencies and banks to the list the following year. "In the hours before Russian troops invaded, Ukraine was hit by never-before-seen malware designed to wipe data—an attack the Ukrainian government said was 'on a completely different level' from previous attacks," the article says.

IS YOUR EVENT DATA AT RISK?

While event-industry firms are likely lower on the list of priorities for Russian cyberattackers, malicious code is called a virus for a reason—it spreads quickly and indiscriminately. Once it attaches to an ecosystem, it can shut an organization, and certainly an event, down. And when malware is introduced, it's almost impossible to confine it to a computer, network, industry, or country. Plus, the global events industry, like many others, has taken a stand against the Russian invasion of Ukraine, which could make it somewhat vulnerable.

While the war in Europe is top of mind for many American firms, it's only the latest threat to their cybersecurity. For example,

- In its Global Risks Report 2021, The World Economic Forum listed cybersecurity failure as the fourth most clear and present danger (behind infectious diseases, livelihood crises, and extreme weather events) the world faces in the next two years.
- More virtual workers attending more virtual meetings has exponentially increased the "attack surface" for would-be cybercriminals.
- A realignment of the workforce due to the 'Great Resignation' has created vulnerabilities in security infrastructure as some former employees take vital institutional security knowledge with them when they go.

CYBERSECURITY VULNERABILITIES TO WATCH OUT FOR

In the current geo-political and post-COVID (work-from-home) climate, event organizations have plenty to keep an eye on:

Busy employees using the same username/password combinations across multiple accounts can become victims of **credential stuffing**, a form of cyberattack whereby hackers use previously stolen combinations of username and password to gain access to other accounts.

Although most major video conferencing and virtual meeting platforms have taken measures to prevent intrusions, hackers may still be able to obtain confidential or sensitive information from participants, which is then sold to another party or made available to the public to damage the company's reputation.

> ***More than 90% of cyberattacks begin as spear-phishing emails, according to Trend Micro researchers.***

Employees working remotely (from the kitchen table or the back of a camper) on their own devices and using their own wireless connections to access an organization's data may not have the appropriate level of device or network security.

Vendors, including technology companies (especially startups that have entered the virtual meeting space more recently) and venues (perhaps not major convention centers or hotels but tents or non-purpose-built spaces, for example) may not have the appropriate network security.

In a presentation SmartSource® sponsored at Staffing World 2021, representatives from Michael Best & Friedrich LLP (Joseph Dickinson), UHY LLP (Jerry Grady), and UHY Consulting Inc. (Richard Peters) discussed current cybersecurity and data privacy threats:

- Ransomware—malware software that holds an organization's data or access "hostage" in exchange for money (usually paid in cryptocurrency)
- Business email compromise—a tactic in which the attacker, posing as someone the recipient knows and trusts, requests a transaction (wire transfer, for example) or information that defrauds the organization
- Spear phishing—an email campaign targeting a specific person or group that exploits recipients' known interests and contains an attachment or link, which exposes the target to malicious software when opened or clicked
- Big data dumps—a massive data breach in which customers' personal information or passwords are stolen from an organization and offered for sale on the dark web
- Security tooling gaps—a possible gap between the tools an organization needs to protect its data, intellectual property, and customers and the tools it has in place

It takes an average of 287 days for security teams to identify and contain a data breach, according to the "Cost of a Data Breach 2021" report released by IBM and Ponemon Institute.

HOW TO REDUCE CYBERATTACK RISK

While cybersecurity is a complex discipline that requires professional management resources, there are some basic steps organizers can take to reduce the risk of attack, such as:

- Require that employees change their passwords frequently.
- Issue secure laptops to remote employees and set up virtual private networks for dispersed employees to use when accessing event-related or organization data.
- Vet software, vendors, and partners appropriately (use internal cybersecurity experts or a managed services cybersecurity firm).
- Train employees to spot spear phishing, business email compromise, and other malicious attacks.
- Take measures to protect the organization from ransomware attacks, including backing up data, keeping software updated, adopting multi-factor authentication practices, restricting employee access to data, and implementing anti-ransomware software.
- Remove departing employee network, social media, and vendor software access.
- Perform a cybersecurity assessment based on guidance, frameworks, and security management systems, including CIS SAT, NIST CSF, and ISO 27001.
- Investigate whether cyber insurance is appropriate for the organization.
- Develop an incident response plan.

NETWORK SECURITY CHECKLIST

The best remedy is to be aware of the risks, take preventative measures, and have a response plan in place. With this checklist, you can take action to prevent the threat of cybercrimes.

Most cybersecurity experts agree that breaches aren't a matter of "if," they're a matter of "when" for every organization.

- ☐ Patch operating systems, 3rd party software, and firmware as soon as updates/patches are released.
- ☐ Install and update antivirus software on all endpoints, and enable real-time detection.
- ☐ Perform backups of all data with encryption enabled during transit and at rest with password protection. Ensure these copies are not accessible for modification or deletion from any system where the original data resides.
- ☐ Ensure that you have implemented and are using multifactor authentication (MFA) wherever possible.
- ☐ Review domain controllers, servers, workstations, and active directories for new or unrecognized user accounts.
- ☐ Use a strong password policy to make sure accounts on the server and the local computer can't be compromised.
- ☐ Enable logging to audit user accounts with administrative privileges, and configure access controls with least privilege in mind. Do not give all users administrative rights.
- ☐ Disable unused ports, especially Remote Desktop Protocol (RDP) ports, and monitor remote access/RDP logs for any unusual activity.
- ☐ Implement SPF, DMARC, and DKIM to stop email spoofing/phishing from your domain.
- ☐ Consider adding an "EXTERNAL" email banner, typically a horizontal yellow banner, to emails received from outside your organization.
- ☐ Disable hyperlinks in received emails.
- ☐ Implement network segmentation, so that all machines on your network are not accessible from every other device.
- ☐ Train users to better identify and prevent cyberattacks, especially phishing attacks.

Talk to the technology experts at SmartSource® to learn more about protecting rented, leased, or owned devices from cyber threats, and keep this Network Security Checklist handy.

QUESTIONS? VISIT THESMARTSOURCE