TIP SHEET:

SUPPLY CHAIN SECURITY CHECKLIST

LMG
SECURITY

NOW IS THE TIME TO TAKE ACTION ON SUPPLY CHAIN SECURITY.

Hackers target suppliers in order to gain access to customer networks, steal data, install ransomware, and more. Here are the steps that every organization should take in 2021 to reduce your security risk:

☑ AIM FOR PROGRESS, NOT PERFECTION

There's no such thing as perfect security, but most organizations have a big gap when it comes to supply chain security. Start by putting a supply chain security plan in place and setting realistic goals that will help you improve.

☑ COLLABORATE

Supply chain security is a global problem, and we need to work together to manage this daunting task. So get involved! For example, you can start by raising the topic in your local infosec meetup, or on your favorite infosec mailing list.

☑ VET YOUR SUPPLIERS

Do you have a supplier vetting program? If not, 2021 is the year! This year, aim to document any informal processes, create templates, and establish more consistent routines. Read our vendor vetting blog for best practices.

☑ PRIORITIZE SUPPLIERS BASED ON RISK

When you conduct vendor vetting, make sure you prioritize your highest-risk suppliers first. Consider which suppliers have privileged access to your IT resources and/or sensitive data, and examine them frequently and carefully.

☑ LIMIT ACCESS

Cut down on your work and your supply chain security risks by limiting suppliers' access to your IT resources and sensitive data to what they really need.

☑ REQUEST THIRD-PARTY SECURITY ASSESSMENT

Often, suppliers already undergo their own third-party security assessments, particularly suppliers that support customers in highly regulated industries. Ask to see summaries or evidence of annual cybersecurity reports. If the supplier can't provide a report, summary, or letter of attestation, it's a red flag.

☑ MAKE SURE YOUR SUPPLIERS VET *THEIR* SUPPLIERS

Fourth- and fifth party supply chain risks are real and have led to costly data breaches. Make sure that your vendors have a process for vetting their own supply chains.

☑ VERIFY SOFTWARE LIFECYCLE SECURITY

As demonstrated by SolarWinds, hacking groups often target software firms to inject malware into multiple customer networks. Ensure that any software provider you work with has a strong software development security program.

☑ UNDERSTAND DETECTION CAPABILITIES

Are your suppliers capable of detecting an intrusion—or would malware sneak by unnoticed? Make sure your high-priority suppliers actively monitor their IT environments and have effective programs in place to detect threats.

☑ REQUIRE TIMELY REPORTING

When suppliers detect an attack, much of the time there is no requirement to report an intrusion unless it affects personally identifiable information (PII). Ensure that supplier contracts spell out circumstances that require notification, required time frames, and consequences for violations.

Supply chain security affects all of us. The problem is too large for any one organization to tackle alone. By collectively pushing for a stronger baseline of standards, we can achieve greater supply chain security and reduce risk throughout the whole technology ecosystem.

Contact us if you need assistance with incident response, proactive threat hunting, or supplier risk management. Our team of cybersecurity experts are here to support you!

LMG Security
145 W Front Street
Missoula, Montana 59802

1-855-LMG-8855
info@LMGsecurity.com
www.LMGsecurity.com