Cybersecurity News

NEWS AND INFORMATION TO HELP PROTECT COMPANIES AND EMPLOYEES

JUNE 2021

Supply chains are increasingly exposed to cyber attacks. To help you understand third-party vulnerabilities and possible risk management solutions, this special edition is exclusively focused on supply chain cybersecurity management.

New guidelines for managing cyber supply chain risks

It is no longer enough for an organization to only protect its own infrastructure alone. Organizations are interconnected and increasingly rely on suppliers to support critical functions. Cyber criminals target the threat perimeter through these suppliers. To help manage these supply chain risks, the Information Technology Laboratory (ITL) at the National Institute of Standards and Technology (NIST) recently published NISTIR 8276 Key Practices in Cyber Supply Chain Risk Management: Observations from Industry.

The combination of digitization and reliance on suppliers to support critical functions creates numerous cybersecurity risks. NIST explains that identifying, assessing, and mitigating cyber supply chain risk is a critical capability to ensure business resilience. This multidisciplinary approach to managing the risks is called Cyber Supply Chain Risk Management (C-SCRM). Based on research that includes expert interviews, development of case studies, and analyses of government and industry resources, NIST developed eight key practices and select key recommendations.

Eight key practices

1. Integrate C-SCRM across the organization
2. Establish a formal C-SCRM program
3. Know and manage critical suppliers
4. Understand the organization's supply chain
5. Closely collaborate with key suppliers
6. Include key suppliers in resilience and improvement activities
7. Assess and monitor throughout the supplier relationship
8. Plan for the full lifecycle

Key recommendations

- Create explicit collaborative roles, structures, and processes for supply chain, cybersecurity, product security, physical security and other relevant functions
- Integrate cybersecurity considerations into the system and product life cycle
- Determine supplier criticality by using industry standards and best practices
- Mentor and coach suppliers to improve their cybersecurity practices
- Include key suppliers in contingency planning, incident response, and disaster recovery planning and testing
- Use third-party assessments, site visits, and formal certifications to assess critical suppliers.

Additional recommendations

NIST suggests more detailed recommendations that map back to its Key Practices on page 13 of its publication. Highlights of these recommendations:

(continued)

DEFINITION: ISLAND HOPPING

An attack that focuses on impacting not only the victim, but also its customers and partners (especially if these partners have network interconnections).

UnionBank®

A member of MUFG, a global financial group

Leadership: Establish supply chain risk councils that include executives from across the organization. Increase board involvement through routine risk discussions and the sharing of performance measurements.

Supplier requirements: Use master lists and service level agreements to establish requirements.

Visibility into supplier cybersecurity: Capture data to understand supplier production processes (e.g., defect rates, causes of failure, and testing information). Know if data and infrastructure are accessible by the suppliers of your vendors. Use third-party assessments, site visits, and formal certifications to assess critical suppliers.

Communication and collaboration with suppliers: Establish protocols for communications, including vulnerability disclosures and incident notifications. Then work with suppliers to understand lessons learned.

Source: National Institute of Standards and Technology (NIST). *NISTIR 8276 Key Practices in Cyber Supply Chain Risk Management: Observations from Industry.* NIST. February 2021. https://csrc.nist.gov/publications/detail/nistir/8276/final.

Manage identity and access to help mitigate third-party risks

Aside from the basics like enforcing least privileges for third-party users and forcing password resets on initial use, consider four ways to mitigate third-party access risks.

1. Establish identities for any people, systems, and things connecting to the enterprise

   Generating an identity for anyone or anything connected to systems creates an inventory of all users, entities, and systems to which they have access. You can then apply controls and technologies to mitigate the risks of unauthorized and inappropriate access.
2. Consider identity broker technology to verify credentials and support authentication requirements

   Cloud identity brokers analyze and verify attributes (e.g., user credentials, device reputation, location) represented in the token and then may invoke strong or multi-factor authentication for added security.
3. Routinely require approvers, sponsors, and other certifiers to verify and attest that users have the correct access and permissions.

   This type of governance on a routine (e.g., monthly, quarterly) basis can also help detect a supply chain attack when incorrect access assignments are uncovered.
4. Implement central management of third-party access for a full view of each user's access

   Most enterprises manage third-party users within line of business applications, but this obscures the view of the multiple systems to which each third-party user has access. Without visibility to the accounts and access rights, there is no aggregate risk view of each user.

Source: McDermott, Dennis. *4 things you can do to minimize cyberattacks on supply and value chains*, Help Net Security. April 8, 2021. https://www.helpnetsecurity.com/2021/04/08/minimize-supply-chain-cyberattacks/.

A secure and more resilient supply chain: three core principles

The World Economic Forum provides three core principles to secure a resilient supply chain.

1. Embed third-party risk management policies and practices in the procurement process and lifecycle.

   Ensure cybersecurity and privacy are woven into the procurement process—from procurement to off-boarding and include compliance requirements in contracts. Then continuously review and optimize security and privacy to address new and evolving threats.
2. Protect the organization's ecosystem with a risk-based approach to third-party assessments.

   Apply risk measurement and ratings tools to identify and rank vendors by risk criticality. This helps establish the measures by which the vendors must take to mitigate risk before entering an agreement. It also sets the frameworks for continuous security monitoring.

   The vendors also benefit because they better understand gaps in their own security postures to further their own cybersecurity maturity.
3. Reduce risks around development, management, and distribution of software and its source code by establishing secure source-code and secure-by-design policies. Base policies on widely recognized frameworks (e.g., NIST framework).
   - Require that all source code written by or on behalf of the organization is not tampered with or contains any known unmitigated security vulnerabilities
   - Restrict source code from dynamically links to third-party hosted source repositories
   - Set parameters for source code storage, transmission (including authorization, access, residency, protection at rest, and in transit) to prevent source code leakage and enable traceability of third-party code
   - Require threat-modeling documentation in the design phase

Embracing a risk-informed cybersecurity approach by assessing vendor security throughout the relationship helps maintain trust with all parties, including business partners and customers.

Source: de Moura, Georges and Blassiau, Christope. *3 principles to reinforce digital trust in supply chains*, World Economic Forum. February 24, 2021. https://www.weforum.org/agenda/2021/02/cybersecurity-hacker-proofing-digital-supply-chains/.

8913482-UB-Online (06/21)