NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Security Guideline for the Electricity Sector - Supply Chain

Cyber Security Risk Management Lifecycle

The objective of the reliability guidelines is to distribute key practices and information on specific issues critical to promote and maintain a highly reliable and secure bulk power system (BPS). Reliability guidelines are not binding norms or parameters to the level that compliance to NERC's Reliability Standards is monitored or enforced. Rather, their incorporation into industry practices is strictly voluntary.

Introduction

The supply chain is one of the biggest sources of cyber security risk for all businesses and government agencies in the world today. For example, the Target, Stuxnet and NotPetya cyber breaches all started in the supply chain. For the electric power industry in North America, supply chain cyber security is especially important because of the serious – and ongoing – attacks by foreign nation-states against critical infrastructure, extensively documented by the U.S. Department of Homeland Security[1] and the Director of National Intelligence[2].

Because no NERC entity has resources that are adequate to mitigate all or even most of the supply chain cyber security threats that it faces, the entity should develop a plan to identify the threats that pose the greatest risk and mitigate those. Therefore, all NERC entities need to identify, assess and mitigate supply chain cyber security threats to their Bulk Electric System (BES) assets.

Identifying Threats

The entity's first objective in the supply chain cyber security risk management (hereinafter "risk management") process is to identify *important* threats to its BES assets. Some of these threats are common to all NERC entities, others to a small group of entities, and yet others to just one entity. Threats that are very unlikely to occur in the entity's environment – or that would produce little impact if they did - should be documented, but need not be considered further.

There are many sources for information on supply chain cyber security threats. These include:

- NERC documents including Cyber Security Supply Chain Risk Management Plans and the EPRI/NERC Supply Chain Risk Assessment: Final Report, and the NERC Cyber Security Supply Chain Risks report.
- White papers by the industry trade associations, including APPA, NRECA, EEI, NATF and NAGF
- NIST 800-161 and NIST 800-171

[1] DHS CISA, "Alert (TA18-074A) Russian Government Cyber Activity Targeting Energy and Other Critical Infrastructure Sectors", available at https://www.us-cert.gov/ncas/alerts/TA18-074A

[2] Daniel R. Coats, Director of National Intelligence, "Statement for the Record: Worldwide Threat Assessment of the US Intelligence Community", available at https://www.dni.gov/files/ODNI/documents/2019-ATA-SFR---SSCI.pdf (ditto)

- NERC CIP-013-1 R1.2.1 – R1.2.6
- Cybersecurity Procurement Language for Energy Delivery Systems, developed by the Control Systems Working Group of US DoE and the NERC CIPC
- White papers developed by the NERC CIPC Supply Chain Working Group (SCWG), such as this one. These as well as other NERC documents about supply chain cyber security are available at https://www.nerc.com/pa/comp/Pages/Supply-Chain-Risk-Mitigation-Program.aspx.
- Best Practices in Supply Chain Risk Management for the Federal Government, developed by the FBI

All of the above documents list mitigations for supply chain cyber security threats, not the threats themselves. However, it is easy to reword these mitigations as threats – although it's important to remember that a statement of a threat must include the impact *to the BES* of the realization of the threat. An example of a good threat statement is "A vendor system that has been granted system-to-system access to a NERC entity's OT systems will be compromised by a malicious third party or a rogue insider and used to exploit an OT system at an entity-owned BES asset. This will result in damage to the BES." This is a restatement of one of the two threats behind the mitigations in CIP-013 R1.2.6.

Assessing Threats

The result of the threat identification step is a list of supply chain cyber security threats that the entity deems worthy of consideration. Because the entity won't be able to mitigate all of these threats, it needs to determine which pose the most risk to the BES. The entity does this by assigning a risk score to each threat, then ranking the threats according to their risk scores.

Risk is a combination of likelihood and impact. The value of each of these two factors must be estimated; their sum or product is the risk score. Because there is no way to reliably assign precise numerical values to the likelihood and impact of a cyber event, the majority of NERC entities will likely assign values of low/medium/high or 1/2/3 to both factors. Other schemes like 1-5 and low/high are also possible.

In determining the likelihood or impact of a threat being realized, the NERC entity can either use fixed criteria or simply estimate based on experience and knowledge. For example, one way to use fixed criteria to estimate likelihood of a threat is to a) identify vulnerabilities that would allow the threat to be realized, b) estimate the likelihood that each of those vulnerabilities will be in place, then c) take the highest of these estimates as the likelihood of the threat itself being realized.

For example, using the threat discussed earlier, one vulnerability that would enable the threat to be realized is "A BCS vendor doesn't have a good patch management program for its own systems." If the likelihood of that vulnerability being in place – for one vendor or for vendors in general – is high, this means the likelihood of the threat itself being realized is high; this is the case no matter the likelihood of any other vulnerabilities that might be identified for this threat.

Once the entity has estimated both likelihood and impact of a threat as low/medium/high, they may assign values of 1/2/3 to both estimates, then add them to get the risk score. The risk score will be in a range of 2 to 6.

After developing risk scores for all the important threats, the entity now should rank those threats from high to low risk, and choose the threats it will mitigate. The entity should try to choose threats to mitigate so that the maximum amount of total risk is mitigated, given the resources available to the entity. This will usually, although not necessarily always, be achieved by mitigating the threats with the highest risk scores. The threats that the entity chooses to mitigate are called Actionable Threats.

Mitigating Threats

Once the entity has chosen the Actionable Threats that it will mitigate, it will determine appropriate mitigations for those threats. These can include mitigations that are applied on an ongoing basis, such as vendor contract language, as well as mitigations that are only applied when there is a particular transaction – e.g. a purchase or installation of a BES Cyber System.

The goal of mitigation is to bring the risk posed by a threat to the low level – e.g. a risk score of 2 or 3, out of a possible range of 2-6. This is achieved by mitigating each of the significant vulnerabilities that could enable that threat to be realized. Returning to the original threat example, significant vulnerabilities could include the vendor's a) ineffective patch management program, b) lack of anti-phishing training, and c) inadequate controls over remote access to vendor systems.

One way to mitigate each of these significant vulnerabilities would be to require the vendor to a) improve their patch management program, b) conduct anti-phishing training, and c) require two-factor authentication for remote access to their systems. This commitment could be documented in an RFP, in a contract, in a letter from the vendor's management, etc. However, no matter how the NERC entity documents the vendor's commitment, the entity also needs to verify the vendor kept its promises.

If these requirements don't provide enough risk mitigation in the case of a particular vendor, or if the vendor refuses to cooperate, the entity should also institute controls of its own to mitigate the risk. Going back to the example, one particularly effective mitigation might be ending system-to-system remote access for the vendor.

Procurements and Installations

Each new product or service procurement or installation should be the subject of a risk assessment. Two powerful tools that aid these assessments are vendor risk score and product risk score. A vendor risk score can be determined for each Actionable Threat, based on – for example – the vendor's responses to a questionnaire. For each Actionable Threat that applies to the procurement, a procurement risk score can be calculated by adding the vendor and product risk scores for that threat. If the procurement risk score is low, the entity may choose not to mitigate this particular Actionable Threat (beyond the level they would in the case of any other procurement). If the score is medium or high, the entity can mitigate the threat by mitigating each of the vulnerabilities that allow the threat to be realized (i.e. reducing each

vulnerability's risk score to low, by reducing its likelihood of being present, its BES impact or both). This same procedure can be followed in the case of installations of procured products.

Updating the Risk Management Plan

All the steps described above should be included in a supply chain cyber security risk management plan. The plan should be updated approximately annually, and perhaps more frequently if new developments warrant doing that. The update should include:

- Identifying significant new threats and assignment of risk scores to them;
- Re-scoring the threats identified previously, based on new estimates of likelihood and impact;
- Updating the list of Actionable Threats based on updated risk scores of both previously-identified and newly-identified threats;
- Identifying significant new vulnerabilities that would enable Actionable Threats to be realized; and
- Reviewing mitigations for each Actionable Threat, to determine whether they are still appropriate. Considerations include whether any current mitigations have proven insufficient or unnecessary, and whether new mitigations have become available that might provide further risk reduction.

Conclusion

The fundamental problem of supply chain cyber security is that no NERC entity has the resources to mitigate all BES risks, or even the majority of them. Following an approach like the one described above is the best way to ensure the entity mitigates the greatest possible total supply chain security risk, given its available resources.