HONEYWELL FORGE

5 SURPRISING FINDINGS FROM OT VULNERABILITY ASSESSMENTS

TABLE OF CONTENTS

5 Surprising Findings from OT Vulnerability Assessments

- Key Missing Layer of Defense
- Dusty Untouched Hardware
- “What Policy?”
- Nowhere to Run to, Nowhere to Hide
- Open Doors, Physically and Digitally

3 Common Questions

- Timing and Assessment Schedules
- Pentesting and Assessments
- “What Do We Do Now?”

Summary of Findings

5 SURPRISING FINDINGS FROM OT VULNERABILITY ASSESSMENTS

The term “vulnerability assessment” can be too broad for engineers and technical personnel responsible for reducing risks across critical infrastructure and operational technology (OT) environments. Yet major security issues are frequently inadvertently introduced when such assessments are not regularly performed, or when they are overlooked due to lack of understanding or deeper clarity. In addition, OT assessments include different steps and deliverables than traditional IT vulnerability assessments, further confusing operational teams. Honeywell personnel who have performed hundreds of OT vulnerability assessments based on in-depth experience across global industrial operations can provide detailed and thorough knowledge to help an enterprise best utilize various types of assessments.

This whitepaper illuminates OT vulnerability assessment findings that may be unexpected or unanticipated, based on Honeywell team experience, to inform technical teams about the real-world practical value derived from these specialized assessments. It also provides broader audiences with current cybersecurity posture information, as they are tasked with lowering high levels of risk in OT environments according to ShieldsUp in the United States and other geopolitical movements. Finally, this whitepaper provides answers to common questions regarding both OT vulnerability assessments and pentesting, two effective procedures designed to identify and mitigate cybersecurity risks when used regularly as part of an overall cybersecurity program.

1 - A KEY MISSING LAYER OF DEFENSE

When OT vulnerability assessments are performed by an objective third party, experts typically review each layer of defense that controls organizational risk and determine relevant physical, technical, administrative or elimination techniques. One common surprise in final vulnerability assessment report findings is that an entire layer of defense is missing all together.

In one real-world assessment, Honeywell resources observed no anti-virus protective layer deployed anywhere across an entire production site. Typically, anti-virus is a fundamental layer and essential for detecting and preventing malicious code. In this case, absolutely no layer was implemented.

Once noted, remediators used a standard out-of-the-box security scan and immediately uncovered a five-year old malicious worm -- on a workstation connected to the process control network. The customer was extremely fortunate that no additional infections were discovered, and the machine was quarantined and ultimately decommissioned. The lack of an essential security layer such as anti-virus was an unwelcome surprise.

OT cybersecurity is focused on defining, measuring and managing what is acceptable risk to an organization. Most notably, and unlike IT, it is weighted toward mitigating or eliminating risks that can cause human or environmental safety catastrophes. A missing layer of defense, whether anti-virus or network segmentation, is a significant finding and one that an experienced OT vulnerability assessor can readily pinpoint before harm is caused.

2 - DUSTY UNTOUCHED HARDWARE

Considering how difficult it is for industrial companies to shut down facilities for maintenance, it might come as no surprise that their cybersecurity is behind the times.

In a recent OT vulnerability assessment that began with customer concerns about performance lags, the routine inventorying hardware step was performed and turned up a visible machine at the plant that was unaccounted for. Layered in dust and undistinguishable to current staff, it clearly had not been touched in years. Staff had no idea about the machine's origins, procedures, or access rights, and had only been told "not to touch it." For security to remain effective, systems typically need frequent patching and updates, thus this machine was a ticking time bomb.

Most companies have such legacy systems, stretching back to 2008 and earlier, and assessors even discover Windows NT in some environments. In some cases, the machines truly could not be touched until another system was prepared and readied for a careful, planned migration. In other cases, high staff turnover resulted in abandoned systems. By performing annual or semi-annual assessments, formerly hidden legacy hardware or operating systems such as these can be identified and a plan of action for mitigation can be prioritized. Without such vigilance, hackers can exploit older systems designed before today's always-on Internet and find ways to reach other layers of the network.

3 - "WHAT POLICY?"

One of the most common assessment categories revealing non-compliance and unacceptable risk levels is the one that appears most bureaucratic: policies and procedures. While many leadership teams focus investments on tangible, innovative technologies and products, in fact, OT cybersecurity policies and procedures are a leading cause of vulnerabilities. In some cases, company personnel don't realize policies even exist. In other findings, the policies do exist, but are not being followed. Either way, the consequence is unnecessary risk.

For OT teams, this can happen due to cyber illiteracy. It is important to distinguish between a cybersecurity baseline and a policy. A baseline is similar to a technical standard. It provides the minimal basic steps or components to comply with a particular regulation or meet legal "best practices" definitions for OT cybersecurity. A policy, however, takes that baseline information and custom-fits it to the organization's needs. Should process control engineers be allowed remote access? If so, under what conditions? If a virus is discovered, who should be called?

Many companies are surprised by vulnerability assessment findings that point to a lack of proper policy and procedure, and this often stems from confusion between baselines and policies. As several prominent Honeywell assessors point out, many damage-inducing cybersecurity issues can be traced back to an issue with policies and procedures. As itemized in assessment reports, there are relatively simple steps companies can take to clean up this category of risk.

4 - NOWHERE TO RUN TO, NOWHERE TO HIDE

Unfortunately, an issue assessors continue to identify is a severe lack of procedures when it comes to emergencies and business continuity. As noted above, a lack of policies and procedures can cause damage, but even worse, untested procedures create a sense of false safety that can come to light in the worst of times. In some cases, for example, OT cybersecurity policies state they will rely on IT business continuity policies as the default instruction set. Yet often, those IT policies offer no specifics when it comes to who OT should call during a cybersecurity incident that causes a plant shutdown. While IT has its vendor's business continuity contacts, OT may be left with a dead end when ransomware affects the operational network.

Instead, plant operators can develop specific OT policies as well as hard copy phone tree instructions printed for safe keeping in the control room. These include 24/7 available experienced vendors who can be called in when disasters strike and if in-house personnel are unable to perform their duties. Workers could be onshore when ransomware strikes the offshore platform, for example, or severe weather or power outages could hamper their plant site access. Part of a proper vulnerability assessment includes roles and responsibilities investigation to learn about these gaps before a real emergency occurs. For trained and prepared cybersecurity professionals, emergencies are typically part of the remediation service and often include 24/7 access, depending on the arrangement.

5 - OPEN DOORS, PHYSICALLY AND DIGITALLY

As assessors walk on site, interview staff, and review documentation for multiple types of checks, another surprisingly common finding is unlocked control room doors and passwords in plain sight. These could be considered open doors, both physically and digitally, in that any malicious actor can readily reach switches or login to critical systems. Through proper training and technical controls, however, these entry points can be better secured on a consistent basis. As assessors like to say, no critical security step should be left to a human remembering to do it. Processes and procedures can be designed and deployed in ways that make it far easier to conform.

Open doors are also surprisingly found in the form of an ADSL line directly connected to a control network, or a hot spot modem device inside the plant. These represent major risks, potentially allowing malicious actors to access and tamper with sensitive controls and settings, such as furnace temperatures or formula compositions.

USBs also represent doors into systems, since malware on memory devices and even certain charging cables can ultimately trigger a plant shutdown. In the case of Operation Copperfield, for example, an oil plant worker inserted a USB with a movie to watch into a company machine, and thus launched malware into the network.

In a more subtle digital-physical finding, one assessment discovered wireless printers throughout the facility, including in the control room. While these were wired, the fact they had wireless capability enabled meant that hackers could exploit them to gain access to the broader wireless network. Also of interest was that company policy had advised no wireless device enablement in the control room, thus the issue also exposed cybersecurity non-compliance.

BEYOND ASSESSING TO PRIORITIZING

These are just five examples, while a typical Honeywell report may include multiple categories of risk types. Beyond assessing and uncovering issues, however, OT vulnerability assessments also serve a greater purpose, independently prioritizing which issues to fix in which order. Is a lack of anti-virus more or less urgent than decommissioning a Windows NT machine? Is it better to use application control or reduce the number of applications in use all together? Should a new plant design include two doors to the control room or just one? These types of prioritization decisions require thoughtful consideration by experienced professionals, and proper assessments include tables and scoring that guide plant operators to make such decisions.

OT cybersecurity decision-making also requires an understanding of scope of work and resources, as there will always be trade-off considerations. How long will fixing each critical vulnerability take? Who will perform the work, and how much will it cost? Armed with complete information, leaders can more confidently and competently mitigate operational risks and stay compliant. They can also better ally with local and global service providers, extending their support circle and access to experienced professionals.

COMMON QUESTIONS

TIMING AND ASSESSMENT SCHEDULES

Vulnerability assessments are one type of assessment and should be performed at least annually, if not more often, depending on local and industry regulations. Assessments are also performed together with key company milestones, such as before a new plant design is approved, before a planned network migration, and often, as new plant assets join the process control network through a business acquisition or change in ownership. Scheduling assessments proactively ensures timely identification and inventory to avoid some of the surprises noted above, and most importantly, to avoid damage to the company, its personnel, and the environment.

PENTESTING AND ASSESSMENTS

A common customer question is when to use pentesting and when to use assessments. Penetration testing, also known as pentesting, is an active test of your OT environment performed by white hat hackers. They probe, email, investigate and otherwise act as an outside hacker would, seeking out gaps and defense workarounds. An assessment, however, takes a particular point in time to detail your cybersecurity status, criticality of issues, and prioritization of remediation steps. Both play an important role.

Pentesting can be performed at any time. In some cases, teams have security concerns, but need professionals to formally prove issues and present findings to the executive team to initiate remediation. In other cases, pentesting is performed after a migration, to verify that procedures went as planned, and to note any remaining gaps. A third use case is regular pentesting to verify security posture, typical of more mature companies. In all cases, assessments are complementary and can be performed in addition to pentesting. For example, once executives see proof of security gaps from a pentesting exercise, they may choose to perform an OT vulnerability assessment. For a migration, assessments might be performed first, then the remediations, then pentesting to determine if security posture was improved. Alternatively, some customers prefer to begin with pentesting to immediately point out issues and prompt rapid action. Both are useful to uncover and act on cybersecurity issues before malicious actors can exploit them.

A regular, disciplined cadence of these professional services also ensures you are continually watching your processes, technologies and people; as the above noted, policies and procedures are not useful unless you enforce and act on them. Pentesting helps identify where there are breakdowns, and where you can add more complexity or difficulty to slow hackers down. Assessments and related remediations are designed to ensure that any active attackers will find it exceedingly difficult to exploit your defenses and detection mechanisms.

"WHAT DO WE DO NOW?"

Another common customer question is what to do when assessments or pentesting unveil problematic issues. First, consider engaging both executives and technical teams ahead of the assessment date. This itself may prompt completion of basic clean-up steps that were lagging. Then, include both teams in final report findings and work together to secure the necessary support and approvals to strengthen your cybersecurity posture. Most teams want to do the right thing. That is far more difficult if they are caught by surprise or not included in the effort up front.

Second, leverage the independent reports. Honeywell vulnerability assessment reports itemize, rank, and detail suggestions for each issue, which helps a customer clear up much of the work scope. An executive summary as well as technical documentation is provided for the relevant leader or team.

Pentesting may also uncover new or unrelated issues. These may fall outside the OT team or require senior leadership education. Working with a trusted provider with substantial experience in multiple OT security areas can expand your team's capabilities to affect cybersecurity improvements. Honeywell teams can assist you in designing and writing policies, for example, based on real events in your plant, and can train teams on the newly documented roles and responsibilities. They can run tabletop exercises for your organization to practice emergency preparedness, and host executives at Cybersecurity Centers of Excellence to view attack demonstrations and current defense strategies. While assessors themselves remain independent in order to best advise on risk reduction, other Honeywell teams can support your journey to advanced OT cybersecurity maturity stages.

SUMMARY OF FINDINGS

Surprising vulnerability assessment findings tell us a lot about cybersecurity weaknesses and make us more aware of real-world issues. Every critical infrastructure facility and operational environment needs a vulnerability assessment and resulting safeguards, just as most facilities need a physical guard standing watch with badge checks at every door. Together with pentesting, table top exercises, assessments play an essential role in providing independent information current to the plant's unique considerations. Honeywell OT cybersecurity teams regularly perform global industrial assessments, including OT vulnerability assessments and pentesting, and can offer detailed and thorough knowledge to assist you in improving your security posture. Assessments are designed to provide the current state of OT cybersecurity, what risks are identified as present, and explanation and prioritization of remediation steps to mitigate risk. Combining assessments with penetration testing diversifies the company's view into potential threats and vulnerabilities, while ensuring a constant eye on processes, people and technologies to help reduce attacker dwell time or exploitation possibilities. Cybersecurity is a perpetual cycle of vigilance, checks and tests. OT cybersecurity assessments performed by independent professionals provide an essential part of that cycle.

Honeywell Connected Enterprise
715 Peachtree Street NE
Atlanta, Georgia 30308
www.honeywellforge.ai

Honeywell