ACCORIAN

CASE STUDY

DRIVING TRUE SECURITY WITH RED TEAMING

Here's how a global leader in power and energy, assessed their readiness for a real-world cyberattack through a Red Team Assessment.

THE CLIENT: A global leader in power and energy boasting a portfolio of nearly 1,000 designed power plants and 2,500+ employees

LOCATION: HQ in USA, with a global network of offices worldwide

INDUSTRY: Power & Energy

SERVICE BRIEF: Our client is a global leader in power and energy, an industry which is expected to reach around USD 3.9 trillion by 2032.

The client has over 120 years of experience offering engineering and consulting services across fossil fuel, nuclear energy, renewable energy, and grid modernization sectors. They boast a portfolio of nearly 1,000 designed power plants and are a vital player in the renewable energy space.

1 THE CHALLENGE FOR THE CLIENT

Although confident in their robust vulnerability management program and existing security controls, the client wanted to assess their preparedness for a real-world cyberattack. They believed their defenses were strong enough to withstand sophisticated threats.

While a robust vulnerability management program is essential, cyberattacks are becoming increasingly sophisticated. Attackers are often employing advanced techniques that are designed to bypass traditional security controls.

2 THE SOLUTION

The Red Team simulated an insider threat scenario, assuming an attacker had already bypassed the external perimeter and gained initial access to the network. Despite a vulnerability management program, the red team identified several vulnerabilities of varied severity within the internal infrastructure.

- A system was discovered to be vulnerable to the infamous **EternalBlue exploit (CVE-2017-010)**, allowing remote code execution and password hash dumping. Password spraying with the dumped hashes proved ineffective.
- The red team then pivoted their attack strategy upon observing support for **LLMNR and NBT-NS** protocols on the internal network. This facilitated the capture of credential hashes over the network. It was further observed that weak password policies allowed users to create easily crackable passwords.
- Cracked credentials enabled **lateral movement** and further access within the network.
- **Overly permissive privileges** and **misconfigured Active Directory rights** allowed the red team to gain administrative access to nearly 4,000 internal systems.

3 OUR GOAL AND THE CHALLENGES

Our goal was to gain access to the Active Directory as a privileged user. The primary challenge was navigating the initial confidence of the client while simultaneously adapting their attack strategy to exploit a complex network environment with multiple vulnerabilities and potential defensive measures. Furthermore, deciding on the most effective approach to achieving the objectives while efficiently utilizing resources and within the allotted time was the key challenge.

4 OUR APPROACH

We proposed a Red Team Assessment methodology that involved a comprehensive assessment of the client's security posture by simulating a sophisticated insider threat attack. We utilized the F3EAD methodology integrated with the MITRE ATTACK framework, employing a systematic approach consisting of distinct phases and identified critical vulnerabilities across various aspects of the network security. We also demonstrated how these vulnerabilities could be exploited to gain significant control.

Our standard approach consisted of six phases:

PHASE 1 – FIND

In the Find phase, reconnaissance activities aimed to identify targets and the crown jewels. This phase set the stage for the subsequent steps in the assessment by laying the groundwork for target selection and strategic goal-setting discussions with the organization.

PHASE 2 – FIX

In the Fix phase, the focus involved intense reconnaissance and intelligence collection against the selected target, delving into the intricacies of the target's systems, and potential points of exploitation. This step was vital in the Red Team assessment process, aiming to attain a level of familiarity with the target that facilitates informed decision-making in subsequent phases of the F3EAD methodology.

PHASE 3 – FINISH

In the Finish phase, the focus shifted to setting plans into action by deploying Tactics, Techniques, and Procedures (TTPs) in a decisive and coordinated manner. This phase was the focal point where planning and reconnaissance transition into practical, impactful actions.

PHASE 4 – EXPLOIT

In the exploitation phase, Accorian acted as the Red Team actor and operationalized the detailed attack plan into action to achieve mission objectives. This phase represented the culmination of strategic planning and the initiation of exploits to realize the Red Team objectives.

PHASE 5 – ANALYZE

The analysis phase involved continuous updates, revisions, and modifications to the attack path and exploitation strategies. Whether an exploit succeeds or fails, the iterative nature of the phase ensures that our testers remain agile and responsive to evolving conditions.

PHASE 6 – DISSEMINATE

In the dissemination phase, raw assessment data was transformed into actionable intelligence, acting as a vital link between the Red Team's activities and the broader organizational context. This documentation provided a comprehensive record of the assessment's results, the next steps for the organization, and fortifying the overall security posture.

5 THE RESULT

While individual vulnerabilities may seem low impact, the Red Team demonstrated how chaining these weaknesses together facilitated a comprehensive attack compromising a significant portion of the internal network. This successful compromise exposed significant security gaps within the client's network.

This case study reinforces the critical need for a proactive approach to cybersecurity and highlights the value of value of red team assessment in bolstering an organization's security posture.

KEY TAKEAWAYS:

- Vulnerability management is crucial, but patching needs to be prioritized and continuously monitored.
- Strong password policies with complex password requirements are essential.
- Least privilege principles should be strictly enforced to minimize damage from compromised accounts.
- Active Directory configurations require careful review and mitigation of unnecessary permissions.
- Regular Red Team assessments are essential to identify and address security weaknesses before attackers exploit them. Security is an ongoing process, not a one-time exercise.

6 SURPRISE IN THE JOURNEY

The client was surprised on two fronts. First, they likely underestimated the threat posed by insiders. Assuming their perimeter defenses were impenetrable, they did not consider the possibility of an attacker already having gained access within the network. Second, the Red Team's success in exploiting various weaknesses exposed vulnerabilities the client wasn't aware of, highlighting the potential consequences of a real cyberattack.

7 WHAT'S NEXT FOR THE CLIENT?

The client has transitioned to a more periodic Red Team engagement model to identify and address new attack paths continuously.

8 WHY ACCORIAN?

Accorian is a leading cybersecurity firm, distinguished by its CREST accreditation, renowned for unparalleled expertise. Our team comprises technology and cybersecurity leaders, ensuring proficiency that exceeds industry standards. What truly distinguishes us is our commitment to tailor-made solutions. Each red team assessment, backed by our remarkable 100% success rate, is meticulously customized to meet an organization's unique needs, ensuring relevance and effectiveness in today's business landscape.

Source: Power Generation Market Size To Hit USD 3.9 Trillion By 2032 (precedenceresearch.com)

ACCORIAN

Focus On Your Business While We Focus On Your Security

info@accorian.com +1 732 443 3468 www.accorian.com