REMOTE SERVICES: ANALYZING THE FINANCIAL EXPOSURES IN INDUSTRIAL SITES

Remote services offer many benefits, such as efficiencies through remote support and maintenance, workforce flexibility, and more, but they also represent significant exposures.

www.denexus.io

Introduction

Remote services offer many benefits, such as efficiencies through remote support and maintenance, workforce flexibility, and more, but they also represent significant exposures. For years, unprotected RDP (remote desktop protocol on default port 3389) has led to many successful ransomware attacks.

It's worth noting that several 2024 studies and reports have reiterated the exposure faced by industrial corporations when deploying and using remote services and remote access solutions:

- DeNexus' partner, Claroty, reports in 2024 that "organizations have far too many remote access solutions deployed within OT environments, creating excessive risk and operational burdens."
- Takepoint Research reviewed the 24 most significant cyber attacks on OT environments. In 17 of the 24 cases, remote services allowed the threat actor to succeed.

This analysis expands on the assumption that remote services represent a significant risk if not adequately managed and secured. This study examines several hundred industrial sites across multiple industries to measure, in monetary terms, the scope of the cyber risks related to remote services. Several aspects of remote services are considered across multiple sectors with operational networks, especially the energy sector, which is under tremendous pressure to strengthen its cyber resilience.

3 QUESTIONS IN FOCUS IN THIS REPORT:

- What is the contribution of remote services to the overall cyber risk posture of industrial sites?
- What are the financial exposures due to remote services?
- How can industrial enterprises deploy remote services and minimize cyber risk?

Methodology

The DeNexus team analyzed risk metrics for more than 200 sites being monitored through its DeRISK cyber risk quantification and management platform. The goal of the analysis is to compare the various Initial Access Vectors as defined by the MITRE ATT&CK® framework for enterprises and ICS

Expected Loss Related to Remote Services

The findings below are based on Annual Expected Loss and the analysis of 254 sites in North America, Europe, and Australia. The data is the output of DeNexus' DeRISK platform on those sites.

For confidentiality purposes, we treated all sites equally and have not conducted any analysis at the company level and their portfolio of sites monitored by DeNexus.

% of Sites impacted by Cyber Exposures Related to Remote Services	92%
% of Sites where Remote Services represent the most significant risk	88%
Average Expected Loss related to Remote Services (site level at 95th percentile)	$223k
Maximum Expected Loss related to remote services (site level, at 95th percentile)	$1.5M

Findings(cont.)

- **8% of the sites analyzed presented no risk exposure to remote services** because they either do not rely on these solutions or have deployed them with all potential risks mitigated.

- **Manufacturing is the sector most exposed to attacks related to remote services,** with an average Expected Loss of $875k compared to less than $220k for the renewable energy sector.

- When analyzing how remote services are leveraged as Initial Access Vectors based on the MITRE ATT&CK framework for ICS, we find that (1) the exploitation of remote services, (2) remote services, and (3) external remote services are ranked #2, #3, and #7 based on the average expected loss across all sites. (The top IAV is phishing). Together, these three IAVs associated with remote services represent the most significant risk.

- The table below clearly shows a pattern on which Initial Access Vectors are most likely to inflict the greatest financial damages if used by threat actors to conduct cyber attacks.

- **Good news:** The top two Initial Access Vectors (IAVs) that could result in the highest financial damages if used by threat actors could be some of the least cumbersome IAVs ro apply stronger cybersecurity measures on.

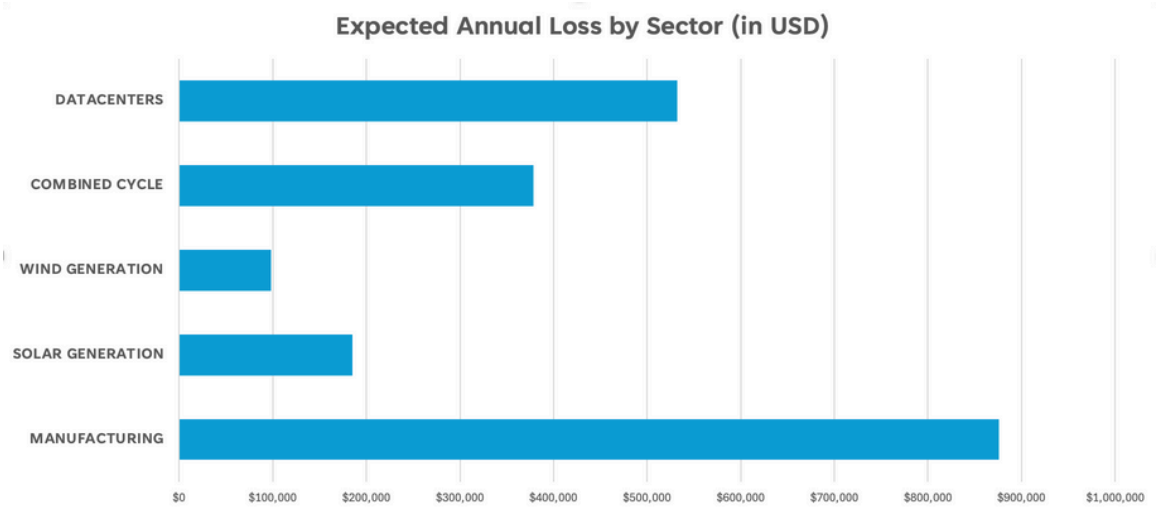
Remote Services Top All Other Initial Access Vectors (IAVs) across the 5 industrial sectors analyzed

	MANUFACTURING	SOLAR GENERATION	WIND ™GENERATION	COMBINED CYCLE	DATACENTERS
Remote Services	1	1	2	1	2
Phishing	2	5	1	4	1
Spearphishing	3	3	3	3	5
Exploit Public-Facing App.	6	2	6	8	6
Drive-by Compromise	4	4	5	2	4
Valid Accounts	5	8	4	7	3
Replication (Removable Media)	7	6	7	5	7
Supply Chain	8	7	8	6	8

Figure 1: Leaderboard for Top IAVs by industrial sectors *(note that the table excluded IAVs that do not represent risks in the sample population analyzed).*

Findings (cont.)

Average Expected Loss for Incidents with Remote Services as Initial Access Vector



Definitions of Cyber Risk Metrics

- **Expected Loss:** The anticipated average financial impact of a cyber risk or set of risks over a specific period. It represents the annualized average of all possible losses weighted based on probabilities and calculated as the sum of the values of all possible losses, each multiplied by the probability of that loss occurring. The Expected Loss changes as cyber risks evolve and needs to be recalculated frequently.

- **Expected Loss %:** Contribution of a specific cyber risk to the overall Expected Loss.

Recommendations

Overall, industrial sites and any site operating Operational Technology (OT) or Cyber-Physical Systems (CPS) should carefully manage remote services and remote access:

1. **Scan for Vulnerability and Patch Remote Services Monthly or More Often:** Remote services, systems, and applications should be routinely scanned for vulnerabilities. When a vulnerability is found, it must be patched immediately because of the high risk related to remote access vulnerabilities. It's important to note that patching remote access differs from patching ICS/OT systems and should adhere to the strictest and most rigorous patching cycles the company can maintain.

2. **Services such as RDP (Microsoft Remote Desktop Protocol) should only be deployed if necessary.** RDP should always be implemented with appropriate security controls, require authentication and not be operated on default ports.

   Protocol Encapsulation: Don't allow direct remote access to the listening TCP/UDP port (e.g., RDP 3389, VNC 5800). Block access to this port until the user establishes a VPN or other pre-authentication. This avoids the situation where the port is always open to any client.
   Intermediary System: Complimentary to protocol encapsulation, one or more intermediary systems, such as VPN firewall, de-militarized network zone (DMZ), and jump hosts, increase the defense in depth and opportunities to detect and respond to suspicious behavior.
   Enforce Strong Authentication: Use Multi-Factor Authentication (MFA) to add an extra layer of security beyond passwords. Implement robust password policies.

3. **Just-in-Time Authorization:** Avoid always-authorized access, where remote users can connect anytime. Technology exists where remote users must submit an access request and have it reviewed by approved personnel in Operations/Engineering at the facility. The approval should be for a limited amount of time.

4. **Regular Password Changes:** Mandate periodic password updates to reduce the risk of compromised credentials.

5. **Account Lockout Policies Linked to Incident Response:** Set up account lockouts after a defined number of failed login attempts to identify brute-force attacks. Lockout is useless if nobody notices because it is enabled again minutes later. If a lockout occurs, investigate immediately.

6. **Implement Network Segmentation:** Separate critical OT networks from IT and external networks. Use firewalls, virtual LANs (VLANs), and demilitarized zones (DMZs) to limit access to sensitive systems. This minimizes the risk of an attacker moving laterally across networks.

7. **Limit Privileges for Remote Users:** Only grant remote access privileges to users who need it for their roles and complement well with just-in-time authorization. Apply the principle of least privilege, ensuring users have the minimum necessary access rights.

Defining Exposures to Remote Services

For this report, we are evaluating the cyber risks related to remote services. We are using the MITRE ATT&CK framework for Enterprise and ICS and are combining three techniques related to remote access and used by threat actors to gain initial access. External remote services allow users to connect to internal network resources from external locations. Examples include VPNs, Citrix, and other access mechanisms

- **The Exploitation of Remote Services (T0866):** Exploitation of vulnerabilities in remote services that threat actors leverage to gain a beachhead into the organization.

- **Remote Services (T0886):** Use of valid credentials (stolen) to penetrate an organization through remote services such as RDP.
  Adversaries may leverage remote services to move between assets and network segments. These services often allow operators to interact with systems remotely within the network; some examples are RDP, SMB, SSH, and similar mechanisms.

- **External Remote Services (T0822):** Threat actor access to VPNs (valid through stolen credentials or leveraging misconfigurations) and other external access mechanisms allowing connection to internal enterprise network resources from external locations or through an exposed service that is missing authentication protection (example: Docker API, Kubernetes API server, Kubernetes dashboard)

The three scenarios described above and as define by MITRE are related. An Exploitable Remote Service is generally an External Remote Service, and both are Remote Services. More specifically:

- **Remote Service = any network-accessible TCP/UDP port.** Cyber assets with a web server or other listening service accepting connections on the network have a Remote Service. Simply enabling a port or service on a computer makes it accessible over the network.
- **External Remote Service = externally accessible + Remote Service.** If a Remote Service is accessible outside the local network, it is considered an External Remote Service.
- **Exploitable Remote Service = vulnerability + External Remote Service.** If the externally accessible service has a CVE vulnerability, it is considered an Exploitable Remote Service.

Why DeNexus?

DeNexus empowers CISOs and risk managers to optimize their cyber risk and cybersecurity programs by quantifying cyber risks in monetary terms and prioritizing risk mitigation based on risk reduction impact.

Using DeNexus and its AI-powered DeRISK platform, security teams can identify cyber risks with the highest potential financial loss and simulate the positive impact of risk mitigation projects. CISOs and CFOs can collaborate to justify cybersecurity investments, including cyber insurance.

DeNexus is dedicated to industrial sectors with OT/ICS environments or cyber-physical systems(CPS), such as energy, manufacturing, hyperscale data center facilities, and transportation. Global 1000 companies in North America and Europe trust DeNexus to optimize their cyber risk management strategy.

References:

- **Claroty: The Problem with Remote Access Tool Sprawl**
  https://claroty.com/resources/reports/the-problem-with-remote-access-tool-sprawl
- **Takepoint Research: Top Industrial Cyber-Attacks Mapped to MITRE ATT&CK Techniques & IEC62443 Controls**
  https://takepoint.co/product/fact-sheet-top-industrial-cyber-attacks-mapped-to-mitre-attck-techniques-iec62443-controls/

Ask for a Demo

https://www.denexus.io/contact

Contact Us

info@denexus.io

DeNexus.io