protiviti®

Face the Future with Confidence

External Exposure Assessment

Securing Environments in the "New Normal"

The global spread of COVID-19 has forced many organizations to rapidly implement a "new normal" operating model where workforces are now entirely remote. This swift and unexpected change brings technology hurdles requiring immediate action by IT organizations across the globe. Attackers target organizations in times of uncertainty and change – and this is no exception. Protiviti has followed and responded to numerous cyberattacks as organizations have implemented changes to technologies and processes to empower their remote workforces.

Protiviti's Security and Privacy team is helping clients quickly assess and understand the risks that exist in their new technology landscapes through a targeted **external exposure assessment**. Our specialized team of Attack and Penetration professionals will simulate real-world tactics in order to quickly identify information that may have unintentionally been made publicly available and to assess the resiliency of your networks, systems, and applications to the types of attacks you are likely facing today.

Our testing approach requires no changes to the existing technology environment and less than an hour of client input once we begin. These simulation results allow organizations to quickly understand points of exposure and address gaps that were created.

Know your external exposures.

Our Approach

Gather Information and Understand Your Environment

Protiviti will conduct information reconnaissance activities and provide detailed information that an attacker may use against the organization, including but not limited to password breach data and exposed system configurations. We will then work with your technical experts to understand the key systems and applications in order to build an attack landscape inventory.

Identify Exposures

Protiviti's Attack and Penetration team will execute an expedited one-week assessment to help you quickly identify and address risks that may be present on Internet-facing systems. The assessment will be executed through a combination of questionnaires completed by your network defenders, vulnerability scanning, and simulated real-world attacks.

Report and Debrief

Leveraging the information obtained from the assessment, we will develop a summary memo detailing the risks identified, potential impact to the business, and guidance for remediation. We will simultaneously work with your technical leaders to conduct a detailed debriefing of the technical gaps identified to empower swift remediation.

External Exposure Assessment

Open Source Intelligence Gathering

- Search open-source and publicly available data to identify information which may be useful during cyberattacks (e.g., employee passwords, email addresses, phone numbers, etc.)
- Perform passive reconnaissance of client networks through third-party data collections and network mapping solutions (e.g., Shodan, Google, etc.)

Entry Point Identification

- Identify and validate systems to be assessed
- Use network mapping tools to identify live systems, open ports, and additional system information (e.g., operating systems - OS, patch levels, etc.)

Identify Vulnerabilities

- Use automated scanning tools to identify potential vulnerabilities on previously identified systems and applications
- Perform manual analysis of identified issues to quantify risk and perform false-positive analysis

Targeted Login Portal Password Guessing

- Leveraging information (i.e., email addresses) obtained during open-source intelligence gathering efforts, perform targeted password guessing attacks against externally exposed (public-facing) login portals

External Controls Assessment

- Through a technical questionnaire, identify client controls which may help to prevent or lessen the impact of inbound attacks. Controls assessed include:
  - Mail and web filtering technologies
  - Internal communication procedures
  - Endpoint security products
  - User access controls
  - Multi-factor authentication

Reporting and Debrief

- Deliver an executive summary memo outlining the identified issues, risks, and remediation guidance
- Deliver a detailed spreadsheet of identified vulnerabilities and gaps with technical remediation steps
- Conduct a debrief session with client management and technical leadership to outline the testing performed and results

Schedule an External Exposure Assessment today by contacting us at TechnologyConsulting@Protiviti.com.

Protiviti.com/TechnologyConsulting

TechnologyConsulting@Protiviti.com

TCblog.Protiviti.com

Protiviti (www.protiviti.com) is a global consulting firm that delivers deep expertise, objective insights, a tailored approach and unparalleled collaboration to help leaders confidently face the future. Protiviti and our independent and locally owned Member Firms provide consulting solutions in finance, technology, operations, data, analytics, governance, risk and internal audit to our clients through our network of more than 85 locations in over 25 countries.

Named to the 2020 Fortune 100 Best Companies to Work For® list, Protiviti has served more than 60 percent of *Fortune* 1000® and 35 percent of *Fortune* Global 500® companies. We also work with smaller, growing companies, including those looking to go public, as well as with government agencies. Protiviti is a wholly owned subsidiary of Robert Half (NYSE: RHI). Founded in 1948, Robert Half is a member of the S&P 500 index.

protiviti®

Face the Future with Confidence