WEBINAR SUMMARY

May 21. 2020

Attacking and Defending a Distributed Workforce

Tim Boswell, Security & Risk Solutions Architect, IT Transformation, ServiceNow
Zach Lanier, IoT Practice Lead, Atredis Partners
Michael Robbins, Principal Risk Consultant, Atredis Partners
Tom Steele, Research Consulting Director, Atredis Partners

KEY TAKEAWAYS

- The shift to a distributed, remote workforce opens new attack vectors.
- Confidential data is at increased risk because most homes lack standard security controls.
- Less structure within the work environment leads to confidential information sharing.
- Traditionally in-person business processes become riskier in remote environments.
- Network availability may not be consistent for remote employees.

in partnership with

servicenow

OVERVIEW

Over the past several years, corporate America has slowly been moving to a distributed workforce, allowing some part- and full-time employees to occasionally work from home. In 2020, as the COVID-19 pandemic reached the US, many businesses shifted to most or all employees working from home.

This rapid shift has changed the risk profiles for many companies, opening up new attack vectors and risks. This is forcing businesses to look at and change day-to-day interactions at both the enterprise and operational levels to defend themselves against these risks.

CONTEXT

Tom Steele, Zach Lanier, and Michael Robbins discussed three emerging threat areas businesses are facing with a distributed workforce. Tim Boswell shared two use cases focusing on how businesses can protect their networks.

KEY TAKEAWAYS

The shift to a distributed, remote workforce opens new attack vectors.

As states issued stay-at-home orders to prevent the spread of COVID-19, the US workforce shifted from one that is primarily office based to one where most office employees have been working from home—and some will continue to work from home for the foreseeable future. The rapid shift to this highly distributed workforce is exposing businesses to three emerging threat areas:

- **Confidentiality threats** focus on how an organization can continue to manage access to confidential data in a distributed workforce.
- **Remote business process threats** revolve around how business processes change when in-person interaction is removed.
- **Availability threats** deal with whether access is consistent when an employee is no longer in a business's office.

> Shifting to a more distributed workforce absolutely changes the risk profile for a company; new attack vectors are opened up.
>
> *Michael Robbins, Atredis Partners*

Confidential data is at increased risk because most homes lack standard security controls.

Within an office building, businesses can implement numerous security controls—both virtual and physical—that help keep confidential data safe. But businesses cannot rely on these same controls when employees are working remotely, making data more vulnerable to attackers.

Table 1: Confidentiality risks with a distributed workforce

Risk	Challenges
Fewer standard controls at home	– Minimal (if any) asset identification; does the employee or employer know what devices are on the home network? – Egress points lack monitoring and controls. – Patching of home network devices lead to an increased attack surface when done sporadically or when systems are not patched at all. – Home wireless security is, by default, weak or non-existent. Open and weak networks are targets for opportunistic attackers, but dedicated attacks against home wireless networks are unlikely.
Shared work/home devices	– Personal, unmanaged devices are being used for work, similar to bring-your-own-device (BYOD). – Devices can be shared across the household using a shared single user account; e.g., parent uses computer for work and child uses it for class. – Securing and monitoring personal endpoints and distinguishing between employee and non-employee activity is problematic.
Internet of Things (IoT)/smart devices	– Difficult to control in enterprise environments, and even more of a challenge in the home office. – No way to verify security of a random, cheap smart device on the employee’s flat home network. – No way to ensure the device is not capturing sensitive business conversations or intellectual property (IP).
Physical security	– Easier to implement and verify physical security in office buildings. – No pragmatic way to verify physical security of workers’ homes. – Is there liability for the company or adjustment for risk tolerance based on employee location, which impacts crime rates? – Unclear if “clean desk” policies, keeping confidential information stored away, matter in the home environment.

> It’s difficult enough to control [IoT devices] in enterprise environments. It’s even harder in a home office, because the enterprise may not be able to verify the security of a random device.
>
> *Zach Lanier, Atredis Partners*

Less structure within the work environment leads to confidential information sharing.

Social engineering tactics, like phone pretexting and phishing, are increasingly likely to work in a distributed environment. The lack of structure makes it even more challenging to distinguish between legitimate calls and emails and risky ones.

Phishing—and the more targeted spear phishing—uses emails to attempt to gain access to systems. The goal of phone pretexting is similar: gaining access to information or systems that can be used to breach the network by having a conversation with an employee over the telephone. Remote employees tend to be more susceptible to phone pretexting than those in an office environment; they feel they can speak more freely as there are no other employees around to overhear a conversation.

Security awareness can help educate remote employees, but operational controls are the best way to protect against these types of social engineering attempts. Documented procedures and processes can help employees recognize how to handle information requests.

Traditionally in-person business processes become riskier in remote environments.

When done remotely, employee onboarding and signature processes open new vectors for attack.

Businesses onboarding new employees are struggling with how to perform employee verification and train remote employees. They also have to prepare laptops remotely for these employees, as well as figure out the fastest, lowest-risk way to get them the laptops.

New employees are also susceptible to phishing and phone pretexting because they are less likely to know their co-workers.

> New employees are always great targets for social engineering. They don't know anybody [in the company] and they're eager to do a good job and not upset anyone.
>
> *Tom Steele, Atredis Partners*

The signature process also becomes complicated and risky when moved from an in-person process to a virtual one. Businesses need to figure out not only which document types can be signed electronically and which cannot, but also how to get electronic signatures, and in some cases, how to get multiple signatures.

Document signing solutions and processes can be helpful for ushering this remote process along, but these tools and processes are also susceptible to social engineering. For example, a customer-facing employee may be convinced to open files from an attacker because it is difficult to validate the customer's identity.

Network availability may not be consistent for remote employees.

Companies have faced numerous network availability challenges as employees quickly shifted from onsite to remote. Businesses have had to adjust their environments so that the network could handle additional remote load. Employees have had to shift to new ways to connect and collaborate with one another, including conference calls and video meetings.

Table 2: Availability challenges with a distributed workforce

Challenge	Questions
Enterprise network bandwidth	– Does everyone get remote access? – How are employees given remote access? Virtual private network (VPN)? Virtual desktop infrastructure (VDI)? Zero trust networks? Dial-up? – Can the corporate network handle the remote load? – What external connections are allowed? Which will be denied?
Connectivity and collaboration	– What happens if an employee's connection dies in the middle of a call? – What happens if a leader drops a meeting; will the meeting end or continue with a new leader? – What happens if someone inappropriately joins a web meeting? – Does the company have standardized collaboration and conferencing platforms, and is everyone using those?

Use Case: Protecting Against Insecure Networks

Remote workers can unknowingly connect to networks that lack security. These networks might be their own home networks that they don't know how to secure and maintain, or they might be a neighbor's WiFi network.

Businesses can take the following actions to safeguard against the risks these networks create.

- Enforce the use of a VPN to connect to the corporate network.
- Integrate endpoint protection with Security Orchestration, Automation, and Response (SOAR) for rapid detection and response to threats.
- Educate workers and provide them with easy options to report security incidents, such as a service portal.
- Empower incident response teams and vulnerability response teams with automation to increase detection and remediation.
- Ensure visibility and accuracy of assets.

> Ensure you have solid policies prohibiting credential sharing, and that these policies are published, that they're understood, and that they're acknowledged by the worker.
>
> *Tim Boswell, ServiceNow*

Use Case: Discouraging Credential Sharing

When working from home, remote workers are more likely to share devices with family members and roommates. While preventing multiple users from using a single device may not be possible, businesses can better protect systems by requiring workers to use their own credentials, and not share the accounts with others in the household.

- Educate on and reinforce Acceptable Use policies with workers.
- Enforce proper credential hygiene.
- Proactively handle vulnerabilities and threats through automated enrichment data.
- Consume, automate, and curate threat intelligence.
- Increase collaboration between Security and IT, especially the endpoint protection and endpoint support teams.
- Ensure accountability of assets.

ADDITIONAL INFORMATION

Listen to and view more on-demand webinars from ServiceNow.

BIOGRAPHIES

Tim Boswell

Security & Risk Solutions Architect, IT Transformation, ServiceNow

Tim Boswell is a Security & Risk Solutions Architect for ServiceNow, and prior to that role he was the Senior Manager of Security Operations within ServiceNow. Tim spent the past four years building, maturing, and optimizing ServiceNow's internal Security Operations Center into a global operation, charged with defending both the corporate enterprise infrastructure and the private cloud infrastructure that hosts customer instances and their data. Prior to ServiceNow, Tim built and managed the security program at Stanford University, and before that he worked as a consultant at RSA Security helping organizations build and improve their security operations and programs. Tim got his start in cyber security as a service member in the US Army and held various positions, mostly centered around incident response and other blue team functions.

Zach Lanier

IoT Practice Lead, Atredis Partners

Zach Lanier leads and executes highly technical software security, network, and application assessments, as well as complex reverse engineering and exploit development projects, focusing primarily on embedded and IoT/IIoT platforms.

Zach has performed extensive security research in a variety of targets, including security products (such as Data Loss Prevention and endpoint/antivirus products), mobile/embedded/IoT platforms such as Android, QNX, BlackBerry, and proprietary operating systems, mobile carrier networks, and esoteric hardware such as electronic voting machines.

Michael Robbins

Principal Risk Consultant, Atredis Partners

Michael Robbins leads and contributes to security projects for Atredis Partners that include system risk assessments, risk management program development, internal control design assessment and process optimization, information security program reviews, and regulatory compliance readiness assessments.

He has relevant experience covering regulations, industry specific and best practice frameworks including CCPA, CIS Top 20, CSA, GDPR, HIPAA, ISO 27001/2, MAR, NIST CSF, SOX, etc. Michael focuses on building lasting relationships with clients, understanding their risks/issues, making actionable recommendations, and helping obtain leadership buy in.

Tom Steele

Research Consulting Director, Atredis Partners

Tom Steele has over 10 years of experience performing adversarial and research-based security assessments. Tom is the author of Black Hat Go and a maintainer of many open-source projects. Tom's focus at Atredis Partners is building and leading offensive capabilities and operations as well as application and software security. Outside of tech, Tom is a black belt in Brazilian Jiu-Jitsu and competes nationally and operates his own gym in Idaho.