JR Coffee's Cyber Security Recommendations

Keith M. Hall
College of Science and Technology, Bellevue University
CYBR515-T302: Security Architecture & Design
Professor Matt Morton
May 28, 2023

JR Coffee’s Cyber Security Recommendations

The following summary identifies threats and vulnerabilities that pose a significant risk of future breaches to JR Coffee's network and the loss of company assets and offers security recommendations for mitigating them. Based on a network security risk analysis, I have concluded that the best solution for mitigating many of the vulnerabilities and threats uncovered is for JR Coffee to implement a zero-trust architecture. Zero trust is said to be the most successful cybersecurity strategy ever devised, and JR coffee possesses most of the network components required to implement one. As a result, the proposed design can be deployed in phases and at an affordable price. However, certain recommendations ought to be addressed immediately. There are configuration flaws that present an immediate threat. Additionally, there are security recommendations you should consider as you expand your business and prepare to move services in the cloud. The attached architecture will serve as a visualization of the proposed architectural changes.

Confidential data is at risk of exposure because of weak network and application layer protocols and unencrypted wireless communication and email.

Point-to-Point Tunneling Protocol (PPTP) is an obsolete method for constructing virtual private networks (VPN) with numerous known vulnerabilities and security flaws. Sensitive information, such as Point of Sale (POS) data, should not be transmitted over a PPTP connection. FTP (File Transfer Protocol) is also flawed. If web developers and administrators are using FTP to move or share files, those files are exposed because FTP does not support encryption, and because its servers use plain text usernames and passwords for authentication, hackers can readily gain the log-in credentials for any

FTP account, as well as the corporate Active Directory if a user logs in to access FTP server.

1. Use the IKEv2/IPsec protocol to implement VPNs. When properly configured, IPsec employs asymmetric and symmetric encryption to deliver speed and the highest degree of security during data transfer.
2. When using FTP to share sensitive files internally or with remote users, run it on top of TLS (Transport Layer Security) to establish a secure, encrypted connection. Consider using a cloud solution like Dropbox for storing and moving massive files or entire directories
3. Use TLS to enable encryption on top of HTTP to create an encrypted connection (HTTPS) whenever your computers connect to the internet via an online server or when developers upload webpages. Enabling HTTPS is also critical to securing your public and private websites. It will safeguard the privacy of users and verify a server's identity to prevent impersonations.
4. Consider encrypting databases that store your most sensitive information assets to defend against both internal and external attacks.

Unencrypted Communications

With “open access” to your wireless network and no logon capability, a hacker with little skill can spy on data sent across all connected devices. But more importantly, since the Wi-Fi connection is a path to the access point, a hacker could install a “back door” on the network’s wired infrastructure.

1) Change the default passwords on wireless access points and implement Zero Trust Access (ZTA). Encrypt data in transit between access points by enabling WPA3 and have users create strong passwords.
2) Activate your Proofpoint subscription so you can automatically encrypt sensitive emails. Use S/MIME for an added layer of security when transmitting extremely sensitive email. In addition to encrypting emails, S/MIME uses public key infrastructure to ensure emails are legitimate, undamaged, and come from the intended sender.

The likelihood of a threat actor successfully installing malicious software to compromise the system is extremely high because network components are out-of-date or unpatched, antivirus and malware protection is not installed, and employees can access web content hackers use to conduct malware attacks.

1) Implement a patch management solution that can automate patching of all network appliances, software, drivers, firmware, and servers. Care must be taken when implementing patch management tools, so I recommend sporadic use of the tool as you plan and prepare to implement a more comprehensive process.
2) Discontinue use of Internet Explorer and any internal apps that rely on it. Instead, upgrade to the most recent version of Windows and look for equivalent applications that work with the latest version. Consider replacing any servers that are more than 4 years old.
3) I recommend you begin migrating to IP6, which is faster and more secure. IPv4 has officially run out of addresses and since IPv6 addresses are the only ones accessible, many of your devices may not operate with your IP6 add-ons. Your infrastructure will need preparation. A specialist can assist you with the transition.

4) Configure firewalls to enable rules, which will allow administrators to specify which traffic is allowed and which is banned.
5) Install anti-virus/malware protection on all virtual servers. To avoid any slow performance issues, choose a solution that uses less CPU and avoid those that are known to slow down machines. Set VMs to use more CPU cores or add extra virtual processors if necessary.
6) Once activated, use Proofpoint to filter emails and guard against spyware and social engineering. The Targeted Attack setting employs an innovative methodology to find, examine, and stop sophisticated threats aimed at your employees. Proofpoint can function as an email firewall, enforcing a set of guidelines that restrict which emails are permitted to access or leave your email network. Use the Smart Search feature to see how messages were handled by the Proofpoint system and locate an email in seconds.

The fundamental policies, procedures, and safeguards for controlling network access are lacking regarding identity management, policy generation and enforcement; and authentication and authorization.

Zero Trust is a high-level network design strategy that assumes that all users, devices, and services attempting to access company resources should not be trusted. As a result, it relies on imposing strong authentication and authorization policies on every device and person before any access or data transmission occurs on a network. For a zero-trust architecture to be implemented, it is essential to combine technologies for identity management, access control, policy creation and enforcement, and continuous monitoring. By implementing the improvements already mentioned and the

recommendations to come, you will be well on your way to implementing a zero-trust architecture.

1) Adopt and enforce separation and least privilege policies to control access to systems and data. Give users no more access or permissions than are necessary to do their jobs.
2) Use the Active Directory (AD) as the main gateway to the network and require a two-step verification process for all access. Be certain to lock out accounts after a defined number of incorrect password attempts
3) Create additional AD organizational units (OU) then configure AD to grant permissions that decide which resources each OU can access. Require a second login for access to the most sensitive resources. Utilize public Key Infrastructure to generate a security token that a user must possess to access those resources
4) AD permission for access to the most sensitive resources should be based on least privilege, activity logs, Security Information and Event Management data, device health, and other parameters.
5) Configure the AD Domain Controllers to serve as enforcement points that enable, monitor, and terminate connections between subjects (users / devices / apps) and resources. I recommend deploying NGFWs on the remaining servers to block unauthorized access.

Continuous Monitoring

To detect insider and other security threats in real time, administrators must have full network visibility by continuously monitoring all users and components within the JR

Coffee network. The goal is to identify potential issues and deal with them as soon as possible.

1) Install an intrusion detection/prevention appliance on the network core that will continually monitor the entire network for malicious activity and prevent it. It would be advisable to install another device off-the-router that forwards traffic to and from the accounting and finance group to detect odd occurrences and generate alerts. Your NGFWs can also add visibility by monitoring user device behavior and interactions with network applications.
2) Install endpoint detection and threat response software on workstations and other endpoints to monitor user behavior and assess security threats.
3) Implement a software platform like Splunk that will let you monitor, search, analyze, and visualize machine-generated logs in real time.

The default configuration for new restaurants poses a serious threat to JR Coffee's network because all employees are given username and passwords for the POS (point of sale) system, the POS software can be minimized, and the host computer used for web browsing.

Keep in mind that POS machines are an extension of your internal network:

1) Employ subnets and a firewall to segregate the POS system from the franchise's guest WIFI and wired network. You should be able to configure the firewall to block any traffic not originating from or being sent to designated IP (Internet Protocol) addresses.
2) Install endpoint protection and response software on POS machines that will encrypt credit data the moment it is entered and when it is transmitted to the

office’s desktop server. This means that regardless of where malware may be installed by hackers, the data is never exposed.

3) Add provisions to future franchise agreements that expressly say that only the store's management may have access to the POS system's username and password. Additionally, consider requiring new owners to take at least 8 hours of security awareness training

Additional Recommendations

Cloud Migration

Moving to the cloud will make your business more scalable, reduce operational costs, and give you access to valuable resources as you expand your business. To secure internal and remote access to shared cloud resources, JR Coffee should consider the following recommendations:

1) Set up a private cloud for enhanced security and host it on premises since you already have the necessary infrastructure in place.
2) Use managed services for your cloud security solution (SECaaS). Select a single vendor that bundles SASE (Secure Access Service Edge) components with SD-WAN (software defined wide area network) capabilities. SASE will allow you to extend your internal zero-trust architecture into the cloud.

Bring Your Own Devices (BYOD) - There are many advantages to letting employees bring their own devices, but there are also many security concerns you should be aware of. Although Zero Trust will help you overcome these issues, I recommend professional consultation for implementing the tools you may need.

Security Awareness Training- Establish a minimum 8-hour security awareness training requirement for all workers, with a focus on phishing and password management.

Conclusion

The threat landscape has changed in recent years. In the past, businesses depended on the "flat network," which allowed access to all corporate applications and data simply by connecting to the network. Users who were able to enter the network were trusted. Legacy security is limited in its ability to address cloud security issues or users who access the network using personal devices from different entry points. Additionally, organizations that accept, transport, handle, or store credit card data must adhere to a set of security requirements mandated by the payment card industry. You can do that with the help of the suggested architecture.

Reference List

Elgan, M. (2023). Why Zero Trust Works When Everything Else Doesn't. Security Intelligence. https://securityintelligence.com/articles/why-zero-trust-works/

Fennelly, L. (2016). Effective Physical Security (5th ed.). Butterworth-Heinemann.

IBM Documentation. (n.d.). https://www.ibm.com/docs/en/informix-servers/14.10?topic=architecture-windows-network-domain

Lake, K. (2022). Does BYOD Fit Into a Zero Trust Security Strategy? JumpCloud. https://jumpcloud.com/blog/byod-zero-trust-security-strategy

Perception Point. (2023, May 31). Zero Trust: From Vision to Reality. https://perception-point.io/guides/zero-trust/zero-trust-from-vision-to-reality/#:~:text=Zero%2Dtrust%20network%20access%20(ZTNA,continuous%20monitoring%20for%20remote%20connections.

Stallings, W. (2017). Network Security Essentials: Applications and Standards.

The Difference Between Threat, Vulnerability, and Risk, and Why You. . .. (2023, May 2). Trava. https://travasecurity.com/learn-with-trava/blog/the-difference-between-threat-vulnerability-and-risk-and-why-you-need-to-know

The Key Components and Functions in a Zero Trust Architecture | Thales. (n.d.). https://cpl.thalesgroup.com/blog/encryption/key-components-function-in-zero-trust-architecture

Vardhan. (2021). Splunk Architecture: Tutorial On Forwarder, Indexer And Search Head. Edureka. https://www.edureka.co/blog/splunk-architecture/

Woock, K., & Anthony, L. (2023). What Is PCI Compliance? A Guide for Small-Business Owners. NerdWallet. https://www.nerdwallet.com/article/small-business/pci-compliance