Fictional Organization

About:

Small, but growing, employee base, with 50 employees in one small office. The company is an online retailer of the world's finest artisanal, hand-crafted widgets.

Requirements:

- An external website permitting users to browse and purchase widgets
- An internal intranet website for employees to us
- Secure, remote access for engineering employees
- Reasonable, basic firewall rules
- Wireless coverage in the office
- Reasonably secure configurations for laptops

Checklist:

- Authentication system
- External website security
- Internal website security
- Remote access solution
- Firewall and basic rules recommendations
- Wireless security
- VLAN configuration recommendations
- Laptop security configuration
- Application policy recommendations
- Security and privacy policy recommendations
- Intrusion detection or prevention for systems containing customer data

Authentication System

First, we'll define some terminology to understand the macro view of our recommendations:

Identification: The idea of describing an entity uniquely

Authentication: Proving *identification*

Authorization: Pertaining to the resources an identity has access to

For identification, and authentication we recommend using Microsoft Active Directory.

Active Directory's default authentication protocol, Kerberos, is a network authentication protocol utilizing the single sign-on authentication concept. **Single Sign-On (SSO)** allows users to authenticate once to be granted access to many different services and applications. The **Kerberos** protocol uses "tickets" to allow entities to prove their identity over potentially insecure channels to provide mutual authentication using symmetric encryption. The specifics of how Kerberos operates can be found in its documentation. I have provided a link to the documentation below:

https://web.mit.edu/kerberos/krb5-latest/doc/

Username / Password Policy

- Emphasize use of password manager
- Usernames/User IDs are case *insensitive* and unique.
- Usernames/User IDs for high security assets could be assigned, rather than user created.
- If using an email address as a username, utilize input validation and ensure the address is deliverable. The only way to do this is to send a confirmation email. This provides a positive acknowledgment that the user has access to the mailbox and is likely but not guaranteed to be authorized to use it. Email verification links should not initiate an authenticated session.
- Password lengths should be no shorter than 10 characters and typically no longer than 128 characters. Longer passwords can create a dos attack on the authentication server which can be mitigated somewhat by choosing scrypt or preferably argon2id over SHA functions for hashing.
- Passwords must include at least 1 of each of the following
  - uppercase character (A-Z)
  - lowercase character (a-z)
  - digit (0-9)
  - special character or punctuation (spaces are special characters too)
- Characters can not be used more than twice (2) in a row (e.g. 111 not allowed)
- Commonly used passwords are banned
- Multiple users must use different password topologies
- Require a minimum topology change between old and new passwords

Multifactor Authentication

We recommend that multifactor authentication is required. **Multifactor authentication** is a system where users are authenticated by presenting multiple pieces of information or objects. Different types of information or objects are categorized into three segments:

- Something you know (password / pin)
- Something you have (ATM / Bank Card)
- Something you are (biometric data)

We recommend either software authentication applications on mobile devices or physical hardware tokens. Short message service authentication (SMS text messages) are not recommended nor is biometric for various vulnerability concerns, privacy concerns, as well as ease of use and flexibility.

Website Security (External and Intranet)

External Website Security

We recommend that the external website server is load-balanced, and proxied behind an nginx reverse proxy. We also recommend long-lived static assets be distributed through a content delivery network (CDN). We believe that a cloud-hosted solution would be preferable, and budget friendly for a company of your size. Be prepared to vett your third-party providors with security questionnaires and request a third-party audit of their security protocols and execution. Your website should be completely certified. We would recommend organization or even extended validation certificates. Extended validation shows the most certificate trust by validating domain ownership, owner identity, as well as a business's legal registration proof.

- A cloud solution will also relieve your organization from the complexity of DNS, DoS and various cross-site scripting (xss, csrf) as security should be managed under your servicel level agreement (SLA).
- Utilizing a managed service providor would improve security as well as offload some of the most important aspects of security; management (patching, updates, miantenence) and monitoring (all forms of logs: access, network, application; intrusion detection / prevention systems).

As an online retailer that processes credit cards, even if you utilize a third-party processor, you must be compliant with the Payment Card Industry Data Security Standard (PCI DSS). A quick PCI compliance guide can be found at https://www.pcicomplianceguide.org/faq/.

Internal Website Security

- Internal website authentication and end-to-end encryption is critical. It is recommended to apply the above authentication protocols in their most secure form. Utilizing the latest TLS standard and hashing functions is mandatory.
- Links to internal websites and access portals should not be indexable nor visible to the public nor non-essential employees. This can be thought of in the context of the **principle of least privilege**and managed using ACLs (Access control lists).
- Critical, high-security assets like databases and backups should be accessed behind **bastion hosts**. Bastion hosts are another layer that restrict connections from certain origins in order to protect critical or sensitive systems or infrastructure.

Remote Access

For remote access, we recommend utilizing a VPN providing end-to-end encryption with perfect-forward secrecy (PFS).

- Access should be restricted to only pre-approved end points by utilizing additional authentication like MAC (media access control) address.
- SSH (secure shell connections) should be never allowed for root sessions and should utilizing symmetric encryption SSH keys with at least a 2048 bit size.

Firewalls

Firewalls should be enabled and configured network-based and host-based. This is a good practice of layered-based security.

- Host-based firewalls protect individual hosts from being compromised when they're used in untrusted, potentially malicious environments, as well as reducing what is accessible to an outside attacker. Host-based firewalls are flexible while only permitting connections to selective services on a given host from specific network ranges. They also help protect against compromised devices on the internal network.
- Dedicated network infrastructure firewalls are the first line of defense for your network.
- Firewall configurations should only be able to be changed by administrators through strict authentication.
- Firewalls should be configured to be a whitelist not a blacklist. Everything is blocked on a whitelist and the administrator can selectively allow access utilizing the least amount of privelege. Blacklists are not

recommended as they allow everything as default and the administrator must explicitly block things in the configuration.

Wireless Security

- Wireless access point access should be protected using at least WPA2-Enterprise 802.1x and the shared secret should follow the above password guidelines.
- Public wireless networks should be segregated from your business network.
- We do not recommend WPS which increases attack surface depending on how WPS is implemented.

VLAN Recommendations

We recommend every segmenet of networking infrastructure is on different VLANs. **VLAN** or **Virtual Local Area Network** is This increases complexity however adds more layers of security. For example, Servers, hard-wired clients, wireless clients, VOIP solutions, printers and print networking, and backup servers should all be on different VLANs.
improve traffic managements

Laptop Security

We recommened that assets be tracked using asset management software like SnipeIT. Additionally, there should be strict use policies. Employees should only use the assets for business related activities. Personal and business use should be physically segragated by device (personl vs business laptop). When connecting to the internet, employees must connect through the companies VPN. Strict authentication is required for these connections. The least amount of services, protocols, applications should be allowed to reduce attack surfaces. Laptops will also be required to be full disk encrypted utilizing both a TPM (trusted platform module) and remote attestation. Implementing key escrow will allow the encryption keys to be securely stored for later retrieval by authorized parties.

Application Policies

Allowing the least amount of applications necessary to complete job duties is recommended. Applications should be monitored and patch as soon as possible with the help of patch management software like Microsoft SCCM or Puppet. It is generally best practice to only support the latest version of a piece of software. However, updates should be thoroughly tested for critical infrastructure. There is always a chance that a new patch could introduce a new bug that might affect the functionality of the device. Application and browser extension permissions should also be throgoughly audited.

Intrusion Detection / Prevention

Networks should be monitored constantly. Utilizing tcpdump or even better, wireshark can help you catch problems and intrusions quickly. Introducing an IDPS (intrusion prevention system) will monitor and analyze network traffic. IDPS opposed to IDS (intrusion detection system) can adjust firewall rules on the fly where as IDS can only detect and alert. This difference could make all the difference in shutting down attacks before they get out of hand.

Security as a Culture and Privacy Policy

Security Policy

Users are a weak link in security. If the right people are compromised, then your entire preventative security systems are for naught. Users should be trained on security practices like never uploading confidential information onto a third-party service that hasn't been evaluated by the company. Employees should understand the importance of strong, unique passwords and why they must trade convenience for security. They must be educated and vigilant for phishing attempts. Incidents will happen. The important thing is to learn from them and solve the root issue. Post-mortems and analysis are not times to assign blame or berate and individual. It is time to promote the importance of security as a culture.

Privacy Policy

It is our recommendation that your privacy policy is in compliance with the new GPDR standard even if you do not currently do business under EU jurisdiction. We recommend collecting the least amount of information necessary taking strict, secure, access and storage measures. Your privacy policy should include the following at a minimum:

- What personal data you collect / store
- How you have obtained the data fairly with the necessary consent requirements
- Inform the data subjects of the specific uses of the data clearly and unambiguously
- Inform the data subjects of their right to withdraw consent at any time
- Ensure data isn't held longer than is necessary and that the data is up-to-date
- Describe how you are keeping the data safe and secure and limitations of access
- Announce the collection of any special categories of personal data and how you are meeting the standards to collect, process, and store it
- If transferring data, explain how you are protecting data in transit