DIY Risk Assessment

# Assets

| Asset | Description | Common Users | Regulatory Impact | Stored | Transmitted |
| --- | --- | --- | --- | --- | --- |
| Credit card | Payment cards used to purchase widgets | Accepting payment | PCI | Encrypted, SQL01 Server | FirstBank – Payment Processing |
| SSN | Employee Social Security Numbers | HR, Payroll | Federal & State privacy | HR-Online Service | HR-Online Service |
|  |  |  |  |  |  |

# Threat Scenarios

| Threat Type | Threat Scenario | Likelihood | Impact | Mitigation Strategy |
| --- | --- | --- | --- | --- |
| External Hacker | Malicious hacker is able to compromise the shopping cart, and steal credit cards | Medium | High | Annual penetration testing, OWASP training for developers |
|  | Website is defaced, creating an illusion of compromise, no records stolen | High | Medium | Backups, vulnerability scanning |
|  |  |  |  |  |
| Insider Threat | Employee steals credit cards | Low | High | Background checks, credit checks, access controls, DLP |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

# Talking about Information Security

| Topic | Questions | Answers / Comments |
| --- | --- | --- |
| Regular Meetings | Does the management discuss Information Security at least monthly? |  |
| Are there meeting notes that can demonstrate agenda and content of the meetings? |  |
| Is there a formal voting process for risk management decisions? |  |
| Security Organization | Is there someone formally responsible for security in the organization? |  |
| Is there a process for escalating security concerns? |  |
| Is there a process for formally accepting risks? |  |
| Do managers / employees know how to bring up or escalate security concerns? |  |
| Do managers / employees know how to report security incidents? |  |
| Policies | Is there an Acceptable Use Policy? |  |
| Is there a Non-Disclosure Policy? |  |
| Is there an Access Management Policy? |  |
| Is there a Password Policy? |  |
| Is there a Data Classification Policy? Is it followed? |  |
| Is there an Incident Handling / Response Policy? |  |
| Compliance | Is someone responsible for ensuring regulatory compliance? |  |
| Have security policies been reviewed for impact on regulatory compliance? |  |
| Is there a formal process for identifying compliance gaps? |  |
| Awareness Training | Do employees receive security awareness training upon hire? |  |
| Do employees receive annual security awareness training? |  |
| Does the training cover security policies? |  |
| Does the training include regulatory requirements? |  |
| Does the training include latest industry trends and emerging threats? |  |
| Is there a process for tracking training attendance? |  |

# Improving IT

| Topic | Questions | Answers / Comments |
| --- | --- | --- |
| Documentation | Is there a logical network diagram? |  |
| Is there a physical network diagram? |  |
| Is there a component diagram? |  |
| Is there a list of all servers / systems / workstations? |  |
| Access Management | Is the AD periodically reviewed for accuracy? |  |
| Are AD groups used efficiently and effectively? |  |
| Is there a process for identifying access exceptions, such as:   * Passwords that don’t expire * Accounts that have never logged in * Expired password accounts * Privileged (domain admin) accounts * Unnecessary user accounts * Unused security groups * Redundant security groups * Empty security groups |  |
| Is there a list of systems that don’t use AD for user authentication? |  |
| Is there a process for reviewing non-AD authentication systems for user accuracy? |  |
| Is there documentation to show security groups used by different applications for authentication / authorization? |  |
| Is there a formal / templated way to provision user accounts? |  |
| Is there a formal / templated way to de-provision user accounts/ |  |
| Are user accounts terminated as soon as no longer necessary? |  |
| Password Management | Are all user passwords changed at least every 90 days? |  |
| Are all system / service / admin account passwords changed at least once per year? |  |
| Is there sufficient complexity required for user passwords? |  |
| Are there extra or enhanced complexity requirements for passwords that cannot be changed at least every 90 days? |  |
| Do you user a multi-user password vault, allowing accountability for all shared credential access? |  |
| Patching | Are servers patched on a regular basis? |  |
| Are critical patches applied within 7 days of release? |  |
| Is someone responsible for monitoring security patches from all technology providers? (Windows, Linux, Databases, Network Devices, Web Browsers, etc) |  |
| Is there a process for identifying missing patches? |  |
| Critical Asset Inventory | Do you maintain an inventory of where critical assets are stored? |  |
| Do you label systems where sensitive data is stored? |  |
| Do you provide additional security considerations for systems hosting sensitive data? |  |
| Configuration Hardening | Do you have templates for deploying servers, workstations, and network devices? |  |
| Have system templates been hardened using CIS or NIST benchmarks? |  |
| Is there a process for identifying any system that is not compliant with hardening standards or requirements? |  |

# Basic Security Considerations

| Topic | Questions | Answers / Comments |
| --- | --- | --- |
| Vulnerability Scanning | Do you perform a periodic external vulnerability scan? (at least monthly) |  |
| Do you perform a periodic internal vulnerability scan? (at least monthly) |  |
| Is the internal scan authenticated? |  |
| Do you have a process / SLA for remediating any exploitable vulnerabilities? |  |
| Do you measure / monitor vulnerability trends? |  |
| Two-Factor Remote Access | Do you require two-factor for remote access to the network? |  |
| Do you require two-factor for access to Outlook Web Access? |  |
| Disk Encryption | Do you encrypt all end-user computer hard drives? |  |
| Do you encrypt all backup tapes? |  |
| Malware Protection | Do you have anti-malware software on all workstations and servers? |  |
| Do you monitor regular updates of virus definitions? |  |
| Do you restrict AV configuration changes? |  |
| Network Security | Do you offer visitors a dedicated wireless network for Internet Access? |  |
| Do you segment visitor wireless network from the main network? |  |
| Do you periodically review all firewall ACLs? |  |
| Do you enforce the same or greater network connection restrictions on the wireless network users? |  |
| Do you require 802.x wireless authentication for all users? |  |
| Do you periodically change wireless pre-shared keys? |  |
| Email Filtering | Do you provide company-wide spam filtering? |  |
| Do you provide company-wide email-based malware filtering? |  |
| Vendor Management | Do you maintain a list of vendors critical to your business? |  |
| Do you indicate which vendors have access to sensitive assets? |  |
| Do you perform due-diligence to ensure vendors are safeguarding your data or access to your systems? |  |
| Do you have the right to audit security of your vendors? |  |
| Do you have mutual confidentiality agreements with all vendors? |  |
| Incident Response | Do you have an incident response plan? |  |
| Is the incident response periodically tested? |  |

# Advanced Security Considerations

| Topic | Questions | Answers / Comments |
| --- | --- | --- |
| Penetration Testing | Do you perform periodic application-specific penetration testing? |  |
| Do you perform periodic external penetration test? |  |
| IDS / IPS | Do you have an IDS / IPS appliance? |  |
| Do you monitor IDS / IPS alerts? |  |
| Is the IPS in blocking mode, or reporting only? |  |
| Automated AD Audit | Do you have mechanisms in place to alert when critical AD group memberships are changed? |  |
| Centralized Logging | Do you have a centralized log aggregator? |  |
| Do you have a meaningful way of searching logs? |  |
| Do you have automated incident identification / critical even alerting? |  |
| Do you forward web access / security logs to the aggregator? |  |
| Do you forward database logs to the aggregator? |  |
| Do you have a SIEM solution, to automatically correlate log events and identify security incidents? |  |
| Network Segmentation | Is the network segmented? |  |
| Do you isolate Internet Accessible servers from all other servers on the network? (DMZ) |  |
| Do you use network segmentation to limit network access based on user’s role? (802.x authentication) |  |
| Do you periodically review network ACL to ensure accuracy? |  |