Online Trust Alliance

SECURITY AND PRIVACY ENHANCING BEST PRACTICES

Released January 21, 2015

To maximize consumer trust and brand protection, organizations need to focus their efforts in the three pillars of online safety: (1) Security, (2) Privacy, and (3) Brand Protection. Organizations looking at these areas holistically are best equipped in protecting themselves and customers from a significant incident. With the onslaught of cybercrime and hactivism, it is no longer "optional" to deploy adequate controls and implement best practices.

OTA's analysis of nearly 500 breaches reported in the first half of 2014 revealed upwards of 90% could have been avoided had simple controls and security best practices been implemented. As the dependency on outsourcing and the cloud has increased, businesses are increasingly relying on service providers to keep their data secure and abide by their privacy policies, further highlighting the need to develop comprehensive security controls and practices.

Organizations can face significant financial and reputational harm as a result of a service provider's data breach and loss incident. Both the organization and service providers must contend with a matrix of obligations governing the disclosure of personal information under federal and state laws and regulations, privacy principles and industry guidelines and standards.

Organizations must put in place appropriate contractual protections with any service provider that has access to their regulated data to: (1) specify the service provider's standard of care and its obligations with respect to the treatment of personal information and sensitive data, and (2) minimize the risks and liabilities associated with a service provider's security breach or the unauthorized use of personal information. Such contractual provisions should stipulate incident notification requirements, material notice changes, and a provision for audits and annual review.

Internal privacy and security teams should at a minimum annually review contractual terms and conditions and consider including applicable best practices as part of a vendor's onboarding process. Updates to this document may be found at https://otalliance.org/2015BestPractices.

SECURITY BEST PRACTICES

Data loss and identity theft occur from an array of increasingly deceptive practices. Social engineering, forged email, malvertising, phishing, and fraudulent acquisition of Internet domains are on the rise. Through a multi-stakeholder input process, OTA has developed a list of recommended best practices, which are easy to implement and manage across all industry sectors. In addition, organizations are encouraged to review other controls including the Critical Security Controls for Effective Cyber Defense, published by the Council on Cyber Security. Combined with OTA's best practices outlined below, these controls are a recommended set of actions that provide specific methods to help prevent, detect and contain today's most pervasive threats.

OTA recommends that all organizations implement the following best practices:

1. **Enforce effective password management policies**. Attacks against user credentials, including brute force, sniffing, host-based access and theft of password databases, remain very strong attack vectors warranting the use of effective password management controls. Best practices for password management include:

    a. Use multi-factor authentication (e.g. one-time PINs) for access to administratively privileged accounts. Administrative privileges should be unique accounts and monitored for anomalous activity and should be used only for administrative activities;

    b. Require users to have a unique password for external vendor systems and refrain from reusing the same password for internal system and personal website logins;

    c. Require strong passwords comprised of an 8-character minimum including a combination of alphanumeric characters, and force password changes every 90 days with limited reuse permitted;

    d. Deploy a log-in abuse detection system monitoring connections, login counts, cookies, machine IDs, and other related data;

    e. Avoid storing passwords unless absolutely necessary and only store passwords (and files) that are hashed with salt or are otherwise encrypted;

    f. Remove or disable all default accounts from all devices and conduct regular audits to ensure that inactive accounts can no longer access your infrastructure;

    g. Remove access immediately for any terminated employees or any third parties or vendors that no longer require access to your infrastructure.

2. **Least privilege user access (LUA**) is a core security strategy component, and all accounts should run with as few privileges and access levels as possible. LUA is widely recognized as an important design consideration in enhancing data security. It also provides protections against malicious behavior and system faults. For example, a user might have privileges to edit a specific document or email campaign, but lack permissions to download payroll data or access customer lists. Also, LUA controls help to minimize damages from exposed passwords or rogue employees.

3. **Harden client devices** by deploying multilayered firewall protections (both client and WAN-based hardware firewalls), using up-to-date anti-virus software, disabling by default locally shared folders and removing default accounts. Enable automatic patch management for operating systems, applications (including mobile and web apps) and add-ons. All ports should be blocked to incoming traffic by default. Disable auto-running of removable media (e.g. USB drives, external drives, etc.). Whole disk encryption should be deployed on all laptops, mobile devices and systems hosting sensitive data.

4. **Conduct regular penetration tests and vulnerability scans** of your infrastructure in order to identify and mitigate vulnerabilities and thwart potential attack vectors. Regularly scan your cloud providers and look for potential vulnerability points and risks of data loss or theft. Deploy solutions to detect anomalous flows of data which will to help detect attackers staging data for exfiltration.

5. **Require email authentication on all inbound and outbound mail streams** to help detect malicious and deceptive emails including spear phishing and spoofed email. All organizations should:
   a. Authenticate outbound mail with SPF and DKIM, including parked and delegated sub-domains;
   b. Adopt a DMARC reject or quarantine policy once you have validated that you are authenticating all outbound mail streams;
   c. Implement inbound email authentication check for SPF, DKIM, and DMARC;
   d. Encourage business partners to authenticate all email sent to your organization to help minimize the risk of receiving spear-phishing and spoofed emails;
   e. Require end-to-end email authentication using SPF and DKIM with a DMARC reject or quarantine policy for all mail streams managed or hosted by third parties.
6. **Implement a mobile device management program**, requiring authentication to unlock a device, locking out a device after five failed attempts, using encrypted data communications/storage, and enabling the remote wiping of devices if a mobile device is lost or stolen.
7. **Continuously monitor in real-time the security of your organization's infrastructure** including collecting and analyzing all network traffic in real time, and analyzing centralized logs (including firewall, IDS/IPS, VPN and AV) using log management tools, as well as reviewing network statistics. Identify anomalous activity, investigate, and revise your view of anomalous activity accordingly.
8. **Deploy web application firewalls to detect/prevent common web attacks**, such as cross-site scripting, SQL injection and directory traversal attacks. Review and mitigate the top 10 list of web application security risks identified by the Open Web Application Security Project (OWASP). If relying on third-party hosting services, require deployment of firewalls.
9. **Permit only authorized wireless devices to connect to your network,** including point of sale terminals and credit card devices, **and encrypt communications** with wireless devices such as routers and printers. Keep all "guest" network access on separate servers and access devices with strong encryption such as WPA2 with AES encryption or use of an IPSec VPN.
10. **Implement Always On Secure Socket Layer (AOSSL**) for all servers requiring log in authentication and data collection. AOSSL helps prevent sniffing data from being transmitted between client devices, wireless access points and intermediaries.
11. **Review server certificates for vulnerabilities and risks of your domains being hijacked.** Attackers often use "Domain Validated" (DV) SSL certificates to impersonate e-commerce websites and defraud consumers. Sites are recommended to upgrade from DV certificates to "Organizationally Validated" (OV) or "Extended Validation" (EVSSL) SSL certificates. OV and EV SSL certificates are validated by the Certificate Authority to ensure the identity of the applicant. EV SSL certificates offer the highest level of authentication and verification of a website. EVSSL provides users a higher level of assurance that the site owner is who they purport to be, presenting the user a green trust indicator in a browser's address bar.
12. **Develop, test and continually refine a data breach response plan**. Regularly review and improve the plan based upon changes in your organization's information technology, data collection and security posture. Take the time after an incident to conduct a post-mortem and make improvements to your plan. Conduct regular tabletop exercises testing your plan and personnel.