CSO Scenario

Albertsons Companies

Jake O’Connor

UAT MS507

Assignment 5

Organization Definition

Albertsons Companies operates over a thousand retail grocery stores, fuel stations, and pharmacies, offers delivery and curbside pickup of groceries, and serves millions of customers a week (*Corporate Profile*). Albertsons Companies also maintains multiple web pages, mobile sites, and apps for iOS and Android. This all makes software development security an extremely important aspect of cybersecurity for Albertsons Companies, as a breach of any of these sites or apps could result in leaked customer data and healthcare information, as well as expose the company to legal and regulatory troubles.

News in Software Development Security

One recent issue in software development security came to light after an India-based cybersecurity vendor called CloudSek released a study revealing that 0.5% of mobile applications contain hardcoded Amazon Web Services (AWS) API keys (Nichols, 2021). The study examined roughly ten thousand applications and found more than forty with easily accessible AWS keys either contained in the source code or saved onto device storage. These API keys are used to securely connect with AWS servers for databases, storage, and many other cloud-based services. Across the forty improperly secured apps, CloudSek estimates over one hundred million user downloads and over five terabytes of cloud storage accessible through these API keys. This all points to a failure in basic software development security policies in the creation of these applications. Even the AWS developer documentation goes into explicit detail on why API keys should never be embedded into the code of an application, and how best to manage the security of AWS API keys.

Critical Software Development Security Concepts

Maintaining software development security principles at Albertsons Companies is important to ensure that customer data is properly secured, and that the organization is not exposed to regulatory fines or a loss of public trust due to a data breach. With multiple different mobile applications and websites exposed to the public, ensuring that these are developed with a secure mindset and well formulated security policies is key to protecting both the company and its customers.

Training and Certification

While there are dozens upon dozens of certifications for cybersecurity professionals at different levels and in different sub-fields, there are far fewer for software engineers that relate to software development security. There are trainings, coding standards, and methodologies important for software engineers to ensure that written applications are secured properly. One such standard is the SEI CERT Coding Standard, developed and maintained by Carnegie Mellon University, which outlines dozens of best practices for software engineers in various languages in order to maximize the software's security from both internal and external threats (*SEI CERT Coding Standards*). Another methodology of note that all software engineers employed or contracted by Albertsons Companies should at least be aware of is defensive programming, such as that outlined in the RedHat Defensive Coding Guide which details several unsecure development practices and best practices for limiting their use in various languages and environments (Weimer et al.). While it's not reasonable to expect software engineers within an organization to maintain a secondary cybersecurity profession in order to guarantee security, it is reasonable to assert that software engineers are aware of software development security principles and develop applications in accordance with security best practices.

Tools and Testing

Software, including both applications and websites, developed by or for Albertsons Companies should all be subject to rigorous security testing both manual and automated in order to ensure that customer and business data is adequately protected. There are dozens of tools used for software security testing, ranging from both open source to proprietary, but most fall into one category: static testing, dynamic testing, interactive testing, or runtime testing (*SAST, DAST, IAST, and RASP: how to choose?* 2019). These different types of security testing tools can be used individually or as part of a greater CI/CD pipeline to ensure that applications are free of obvious security flaws before they can be released to customers. By using all these tools in concert, organizations such as Albertsons Companies can help to ensure that the software and services they create are free of detectable vulnerabilities with little additional effort and can more effectively respond to potential security issues earlier than if no tooling were in place.

Secure Development Lifecycle

One of the best ways in which companies can ensure that their software and services are free from security defects is to embed security principles into the entire development process. The Secure Development Lifecycle (SDL) is a structured approach to application security best practices from design through deployment and eventual sunsetting (*How to approach secure software development* 2020). Secure development lifecycle methodologies reduce both the risk to a company and the cost of development by preventing errors and vulnerabilities earlier in the development process.

References

CISSP Domain 8 Overview: Software Development Security. Infosec Resources. (2017, July 16). https://resources.infosecinstitute.com/certification/cissp-domain-8-overview-software-development-security/.

Corporate Profile. Albertsons Companies: Corporate Profile. (n.d.). https://investor.albertsonscompanies.com/corporate-profile/default.aspx.

Foster, S. (2020, July 15). *Guide for Software Development and Software Security*. Perforce Software. https://www.perforce.com/blog/kw/software-development-and-software-security.

How to approach secure software development. Positive Technologies. (2020, February 25). https://www.ptsecurity.com/ww-en/analytics/knowledge-base/how-to-approach-secure-software-development/.

Nichols, S. (2021, May 6). *Popular mobile apps leaking AWS keys, exposing user data*. SearchSecurity. https://searchsecurity.techtarget.com/news/252500361/Popular-mobile-apps-leaking-AWS-keys-exposing-user-data.

SAST, DAST, IAST, and RASP: how to choose? Positive Technologies. (2019, August 2). https://www.ptsecurity.com/ww-en/analytics/knowledge-base/sast-dast-iast-and-rasp-how-to-choose/.

SEI CERT Coding Standards. CERT Secure Coding - Confluence. (n.d.). https://wiki.sei.cmu.edu/confluence/display/seccode/SEI+CERT+Coding+Standards.

Weimer, F., Mavrogiannopoulos, N., & Relyea, R. (n.d.). Defensive Coding Guide. http://redhat-crypto.gitlab.io/defensive-coding-guide/#_programming_languages.