Keegan Heaton
NTS201
10/07/2023

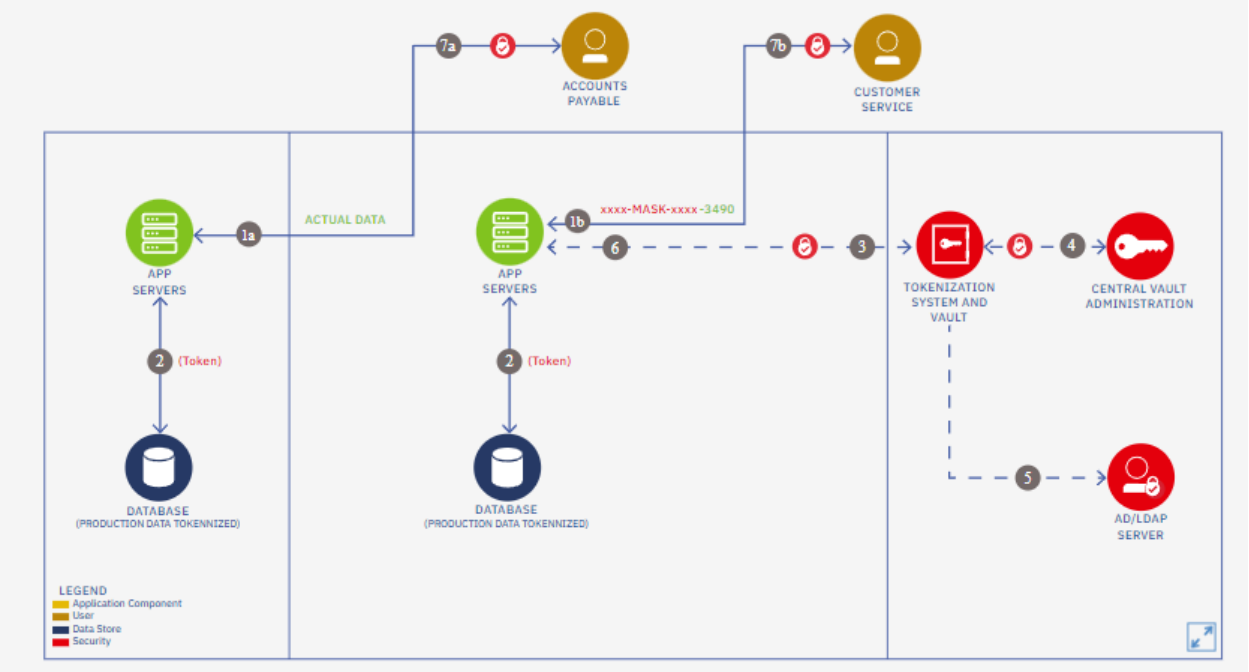
T-Mobile Security Analysis and Security Plan Documentation

In the most recent T-mobile data exposure, happening in September of this year, fewer than 100 customers had their personal and financial information exposed during an error triggered by an overnight update. I'm going over what changes should be made to ensure vulnerabilities like these are avoided.

Technical Control: Automated Testing, Data Encryption, and Tokenization

To combat these software anomalies that appear after updates, T-Mobile should implement IEEE 1044 standardized software testing procedures. (IEEE SA, n.d.) This procedure will automatically report any software anomalies regardless of when or where the error originated from. Additionally, T-Mobile should implement scripts that simulate real-world situations that reflect the update downtime and ensure any vulnerabilities that are discovered in the simulation are correctly handled and responded to. Continuous integration and continuous deployment pipelines can automate the testing process and automatically test the updates before they are implemented. To better understand, Continuous Integration is a dev operation where developers merge their code changes into a repository after which tests are run. (Amazon Web Services, n.d.) Continuous Deployment is the automatic release of developer changes into the production environment after it has passed all configured tests for risk management. (IBM, n.d.) To ensure the security of customer data, all the data should be encrypted at rest, not being used, and while in transport. T-Mobile should use encryption Algorithms like AES(Advanced Encryption Standard) and TLS (Transport Layer Security) to better protect the data altogether. T-Mobile can also use Tokenization. To better understand, Tokenization is a security technique that substitutes the sensitive information in a database for a token.(Smith, n.d.) This token has no

immediate value but acts as a key to the data it substituted and runs authentication to make sure the user has the appropriate access. This adds another layer to the data so that when a breach does happen data isn't immediately available to the malicious actors.



This visual representation shows how Tokenization works. Essentially, Once a request for the data comes in, the token and user ID are given to the Central Vault Administrator which decrypts the key based on the information the AD/LOAP server provides. Then, depending on the level of clearance the user has, the result will be sent to the user. If the user doesn't have the right level of authority, then all they receive is useless values and numbers. The graph and a more detailed summary are available in the citations. All credits go to the author Amy Smith and this graph was only used for further explaination. (Smith, n.d.)

Operational Control: Access Control, Privilege Management, and Regular Employee Training

To better stabilize Operation Controls, T-Mobile should implement role-based access control (RBAC) and principles that restrict access to consumer data. (Zhang, 2023) Access to consumer data should only be given to specific job roles that consider the data a necessity to operate. T-Mobile should also implement two-factor authentication (2FA) to add an extra layer of security for interior systems and sensitive customer information. Continuous Employee Training about modern data security practices and putting an emphasis on their role of integrity and security will help with the general understanding of customer data. Showing different types and styles of content will help employees understand the risks around bad security habits. (Knowbe4, n.d.)

Management Control: Incident Response Plan and SEC Reporting Compliance

Developing and maintaining a robust Incident Response Plan that outlines the step-by-step process to handling a data breach is essential to the reduction of compromised data. This includes a clear chain of command, highlighting the responsibilities of each role, outlining the necessary steps to communicate damage for Attack Threat Modeling, and listing the procedures to quickly recover data and contain any aftermath. IRPs should also have a sunset clause so that a deadline for optimization is clear and IRPs can be continuously improved.

T-Mobile should also put more detail into their SEC reports when dealing with cyber security breaches. SEC Guidelines require companies to report any material losses and cyber security breaches to investors, governing bodies, and the public. (Securities and Exchange Commission, 2023) T-Mobile should follow the regulations more closely and put more detail into

their report to help public confidence in the brand. Following closer to the regulations will also make data on breaches easier to collect and in-depth analysis will be more available.

The T-Mobile data exposure serves as a reminder of the importance of data security. By implementing these recommendations to the current technical, operational, and management control models, T-Mobile can effectively reduce the risk of large breaches and automate responses for inevitable vulnerabilities. Additionally, the public's confidence in T-Mobile can remain strong in times of evolving malicious actors.

Citations

Amazon Web Services. (n.d.). What is Continuous Integration? – Amazon Web Services. Amazon Web Services, Inc. https://aws.amazon.com/devops/continuous-integration/

Balakrishnan, P. (2023, October 6). T-Mobile Data Exposure Incident: My Analysis and Detailed Technical Recommendations. Linkedin.com. https://www.linkedin.com/pulse/t-mobile-data-exposure-incident-my-analysis-detailed-balakrishnan/

BitDefender Enterprise. (2021, December 1). What's Included in a Security Blueprint? Bitdefender Blog. https://www.bitdefender.com/blog/businessinsights/whats-included-in-a-security-blueprint/

Blair-Frasier, R. (n.d.). | Security Magazine. Security Magazine | The business magazine for security executives. https://www.securitymagazine.com/articles/99300-t-mobile-confirms-second-data-breach-in-2023#:~:text=On%20April%2028,%20T-Mobile,most%20recent%20incident%20affected%20836.

IBM. (n.d.). What is continuous deployment? | IBM. IBM in Deutschland, Österreich und der Schweiz | IBM. https://www.ibm.com/topics/continuous-deployment

IEEE SA. (n.d.). IEEE Standards Association. IEEE Standards Association. https://standards.ieee.org/ieee/1044/4607/#:~:text=IEEE%20Standard%20Classification%20for%20Software%20Anomalies&text=This%20standard%20provides%20a%20uniform,,%20product,%20or%20system%20lifecycle.

Knowbe4. (n.d.). Ultimate Guide: Security Awareness Training | KnowBe4. Security Awareness Training | KnowBe4. https://www.knowbe4.com/security-awareness-training

Longbottom, C. (2021, April 22). The pros and cons of CI/CD pipelines | TechTarget. Software Quality. https://www.techtarget.com/searchsoftwarequality/tip/The-pros-and-cons-of-CI-CD-pipelines

Organimi. (n.d.). T-Mobile's Organizational Structure [Interactive Chart] Organimi. https://www.organimi.com/organizational-structures/t-mobile/

Securities and Exchange Commission. (2023, July 16). SEC.gov | SEC Adopts Rules on Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure by Public Companies. SEC.gov | HOME. https://www.sec.gov/news/press-release/2023-139

Smith, A. (n.d.). Protect sensitive data by using tokens. IBM in Deutschland, Österreich und der Schweiz | IBM. https://www.ibm.com/cloud/architecture/architectures/security-data-tokenization-solution/

Zhang, E. (2023, May 5). What is Role-Based Access Control (RBAC)? Examples, Benefits, and More. Fortra's Digital Guardian. https://www.digitalguardian.com/blog/what-role-based-access-control-rbac-examples-benefits-and-more