Emtech Group, Inc

QMT

Security Measures to Prevent Overwhelming Odds

QMT: Security Measures to Prevent Overwhelming Odds

Contents

Executive Summary

The world of life insurance and annuities is dynamic, and data driven. Insurers handle sensitive personal, financial and confidential information, making this sector a prime target for cybercrime. Furthermore, as the industry continues to shift towards digitalization to deliver high-quality products, cybercriminals are exploiting vulnerabilities in integrated platforms to gain access to sensitive data. As a result, cyber-attacks against this sector have been steadily increasing in recent years[1].

Protecting the sensitive data of policyholders is of utmost importance. Several cybersecurity regulations and compliance requirements have been established to safeguard customer information and ensure the stability of the insurance industry. The insurers must comply with HIPAA regulations in the U.S., and GDPR to maintain business relations with EU citizens. In addition, they must conduct their IT and business operations in a controlled environment governed by a set of standards, processes, and structures to facilitate internal control. At least every year the Chief Information Officer (CIO) must renew SOC 2 attestation to the Board of Directors that they have the organizational ability to store and process their customers' data securely. Despite all the effort put into regulation compliance, security policy, and implemented solutions by the insurer, they may not be effective in preventing successful cyberattacks if the insurance carriers' third-party technology providers do not prioritize secure product development and deployment.

Emtech QMT is a high-performance model-based quality engineering software solution for validating the insurance value chain. QMT automatically generates test cases and test data along with test scenario execution. By testing the end-to-end process of life insurance systems, and the integrations between them, carriers can drive quality into product launches and eliminate embarrassing errors experienced by distributors and customers post-launch. Apart from functional enrichment, Emtech is committed to protecting and safeguarding sensitive data that it encounters during its operation. This white paper outlines the development processes that Emtech has undergone, as well as the security features that QMT has incorporated. Therefore, this paper provides peace of mind to customers regarding QMT's security.

[1] The insurance industry cyber crime report: recent attacks on insurance businesses.

Introduction

Over the past decade, the insurance industry has embraced digital transformation, not only to meet evolving business needs but also to ensure top quality as they launch new products more efficiently. To accommodate this transformation, insurance companies are adopting digital technologies and relying upon third-party providers; subsequently, cybercriminals are attacking insurers by exploiting the vulnerabilities of the insurance value chain. The SolarWinds hack[2] is a prime example of the damaging effects of cyber-attacks. The attack on a single supplier had serious ramifications for governments and businesses worldwide. The management of cyber risks in the value chain relies heavily on suppliers' cyber resilience. The following sections will discuss the effects of cyberattacks on insurance companies, the challenges that insurers face in managing value chain risks, what Emtech has done during its development and deployment processes of QMT, and finally, the security measures Emtech has integrated into QMT to safeguard sensitive data.

Cyber Attacks and the Insurance Sector

Life Insurers collect, process, and store a wealth of personal, financial, and confidential data. This industry is also interconnected with other financial institutions as well as health networks. As a result, cyber-attacks on insurers have a wide impact, not just on the companies themselves, but also on the policyholders and businesses they are interconnected with. In 2023 alone, several insurance companies have faced cyber-attacks, including Sun Life, which was attacked via Pension Benefits Information LLC in June; Prudential Insurance, which affected more than 320,000 customer accounts in May; New York Life Insurance Company, which affected 25,700 accounts during the same days as Prudential[3]. These insurance companies were all affected by the MOVEit file transfer cyberattack.

[2] The untold story of the boldest supply-chain hack ever.

[3] Insurance companies have a lot to lose in cyberattacks.

Some of the consequences that result from cybersecurity incidents in the insurance sector include:

- Financial loss due to data breaches and theft of sensitive customer information.
- Damage to the company's reputation and loss of customer trust.
- Legal and regulatory penalties for failing to protect customer data.
- Disruption of business operations and loss of productivity.
- Increased costs for implementing new security measures and recovering from the incident.
- Potential lawsuits from affected customers or third parties.
- Loss of competitive advantage as customers may choose to switch to more secure insurance providers.

Observation shown that both internal and external sources, such as third-party technology providers have been exploited to initiate an attack on insurers. Hence, a collective effort is required to triumph over such overwhelming odds.

Challenges to Mitigate Value Chain Attack

By compromising a trusted component or software within the value chain, cyber attackers can infiltrate the target insurers and their networks. According to a recent study conducted by Reversing Labs[4], 98% of respondents stated that security issues in the software supply chain pose a significant risk to their business. Insurance companies, like other organizations, are unable to mitigate the value chain risks alone due to the lack of control they have over their software suppliers. For example, software can be injected with malicious code before being used if the supplier does not follow secure software development practices. In addition, identifying software vulnerabilities also requires the right tools, time, and expertise, which the insurer may not have. Cybercriminals can exploit a zero-day vulnerability in the interim between the time the issue is discovered, and the patch is released by the vendor. Therefore, the cyber resilience of third-party software suppliers is crucial in developing a comprehensive cybersecurity strategy.

[4] Nine out of 10 companies detected significant software supply chain security risks in the last 12 months.

QMT: Security Standpoint

Emtech recognizes that cybersecurity is a shared responsibility and has implemented measures to ensure the security of QMT and its application. With access controls and a secured model relational database, QMT implements security for a controlled environment that supports SOC 2 attestation and HIPAA compliance. Best practices were followed during the development of QMT, and adequate measures have been taken to promptly address any newly discovered vulnerabilities.

A. QMT: Functional Overview

QMT is model-based testing software. QMT allows the App Dev team to shift left by finding defects earlier, thereby reducing the QA cycle. Using QMT, insurance carriers map out their systems and then create and execute automated test cases that cover the full map. This process starts with model creation where users drag and drop nodes based on the business logic to create a diagram of the flow representing their end user's potential actions. QMT also has a model configuration manager that allows users to select specific questions and values from an existing model to create a new model to test a specific scenario. Users then save the model. The model is saved in the predefined location (in the model folder under a specific project). The next step is to generate test cases from this model file. A test generation plugin can be accessed from the menu bar to automatically generate test cases from the model file, which creates a database of test cases and test data. Finally, this database is read, and a test execution plugin executes each test case and generates a report.

B. QMT: Security Overview

Throughout its operation, QMT produces several artifacts: models, test cases, test data, and reports. These artifacts can be saved and shared with different stakeholders. It is unlikely that customers would use personally identifiable information to generate the model. However, Emtech has implemented proper security measures to protect these artifacts so that attackers are not able to retrieve personal information from these artifacts. Various security features such as screen lockout, user activity monitoring, and authentication have been integrated into QMT to protect it from internal threats. Along with following best practices during the development and deployment of software, Emtech has also taken steps for the maintenance of QMT to strengthen security and regulatory compliance.

The following details the processes and practices Emtech has implemented during the development and deployment of QMT, as well as the security features integrated into QMT to protect its application.

Secure software development

In the software development process, Emtech has adhered to the National Institute of Standards and Technology (NIST)-Secure Software Development Framework (SSDF), for protecting QMT from all kinds of unauthorized access and tampering. Emtech has implemented least privilege access to the code repository to protect all forms of code from unauthorized access and tampering. The development team uses version control features and commit signing to track all changes made to the code with accountability to the individual developer. Throughout the development process, the developers have adhered to secure coding practices.

Security testing

Emtech has conducted security testing in-house and by third parties following the development process. Static code analysis has been carried out during the development of QMT to help the developer identify vulnerabilities early by comparing the code to industry standards. QMT uses Mypy, Pylint, and Flake8 for code analysis. Furthermore, Python Poetry is used to declare and manage library dependencies of the code. The development team uses GitHub code scanning features to identify potential security vulnerabilities. When GitHub flags an issue, the issue is fixed immediately, and then poetry.lock file is updated using the update command.

Authentication and screen lockout

The insurance sector faces cyber risk from both internal and external sources. To prevent unauthorized access to the software from any internal threats on the insurers' premises, authentication features have been employed. Users need to be authenticated (i.e., have an ID and password) to access the application. QMT has a customized screen lockout feature. When the screen is inactive for a certain period, it locks, and the login window appears.

Code signing process

A cyber threat actor may compromise the software before the supplier sends it to customers. Emtech uses digital signing certificates to sign the executable code and supporting documents to protect the software from malicious alterations and malware attacks. Code signing ensures our customers that the software is authentic and has not been tampered with.

Encryption

To ensure sensitive data is not accessible by unauthorized users, QMT has employed industry-accepted encryption techniques during data transmission and database encryption. All data in transit and at rest will be encrypted to protect the sensitive information. Emtech R&D will closely monitor the changing cryptographic landscape and update the software to address new cryptographic weaknesses as they emerge as well as implement best practices.

Logging for tracking user activities

QMT is equipped with a logging system for monitoring users' activities and capturing error conditions that it encounters before crashing. While logging sufficient information for troubleshooting, QMT ensures that sensitive data is not exposed or stored in logs. Proper log management practices such as secure storage, access control, and log rotation are also considered in QMT development to protect the integrity and confidentiality of logged data.

Software patching

The cyber attackers are continuously investing their time and efforts to exploit the vulnerabilities of the systems. Emtech's vulnerability management team is responsible for reviewing, analyzing, and testing the software's code to identify and confirm the presence of previously undetected vulnerabilities. In addition, the team monitors national vulnerability databases and reviews software composition data to identify and confirm new vulnerabilities. Accordingly, QMT is patched regularly to keep it free from any vulnerabilities.

Recommendation for Emtech QMT Customers

Insurance carriers should implement necessary measures to safeguard their systems and networks to ensure the proper functioning of QMT. These measures may include, but are not limited to:

Updating operating system

It is important to update the operating system and applications as soon as new releases are available. Most updates include security fixes to prevent hackers from accessing data.

Updating web browsers

It is crucial to ensure that all browser updates are installed, and browser security settings should be reviewed regularly.

Installing antivirus

To keep computers free from infection, it is important to install and run antivirus software. Regular virus scans should be scheduled and performed to ensure the ongoing security of the computer. Automatic updates are available on some advanced antivirus programs, which further protect systems that emerge every day.

Using a Firewall

It is imperative to make sure that a Firewall is enabled and configured correctly before going online. Also, the Firewall policy must be tested regularly.

Using strong passwords

To ensure security, a strict password policy must be implemented, and users should be motivated to create robust passwords and update them frequently.

Ignoring spam

It is crucial to avoid installing software from unfamiliar sources, or any suspicious software. Users should be suspicious of unsolicited emails and must not click on links or open attachments that accompany them.

Conclusion

Supply chain cyber-attacks pose a major threat to organizations across various sizes and industries. The life insurance industry is particularly vulnerable due to its size, scope, and the significant amount of sensitive data it collects, manages, and stores to operate effectively. As cyber threats continue to evolve and become more sophisticated, all parties in the value chain must take a proactive and comprehensive approach to mitigate cyber-attacks and ensure the integrity and resilience of the interconnected digital ecosystem.

As a member of the value chain, Emtech recognizes its responsibility for security and is committed to ensuring the security of QMT and its applications. Emtech offers customers peace of mind by implementing secure software development and delivery practices recommended by NIST and organizations such as BSA, OWASP, and SAFECode. It has integrated various security features into QMT, such as screen lockouts, monitoring user activity, and authentication. Emtech also advises its customers to implement sufficient security controls in the environment where QMT operates, as no security procedure is completely immune to compromise.

About Emtech Group, Inc.

Emtech Group Inc (ETG) is the leading provider of enterprise software quality engineering solutions for validating insurance carrier value chains. Our customers are enabled to deliver quality products while avoiding the expensive and embarrassing consequences of the exposure of production defect leakage.

Contact Information

For more information, or to see how QMT changes the way quality engineering is done, contact Emtech Group at **sales@emtechgroup.com**