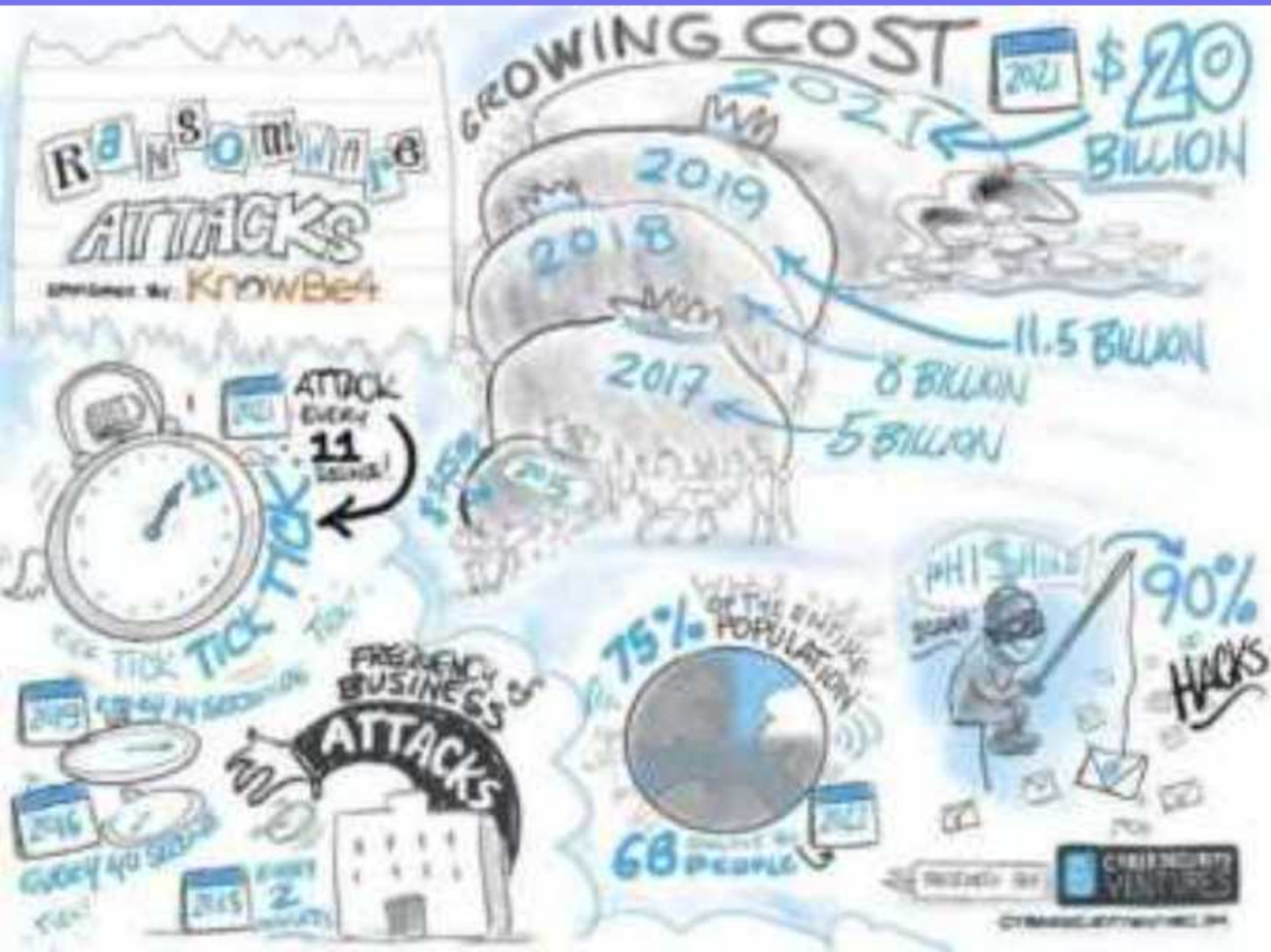
FOCUS ON SECURITY: WHY DID INSUREDMINE INVEST IN PENTEST

INSUREDMINE

WHAT IS A PENTEST?

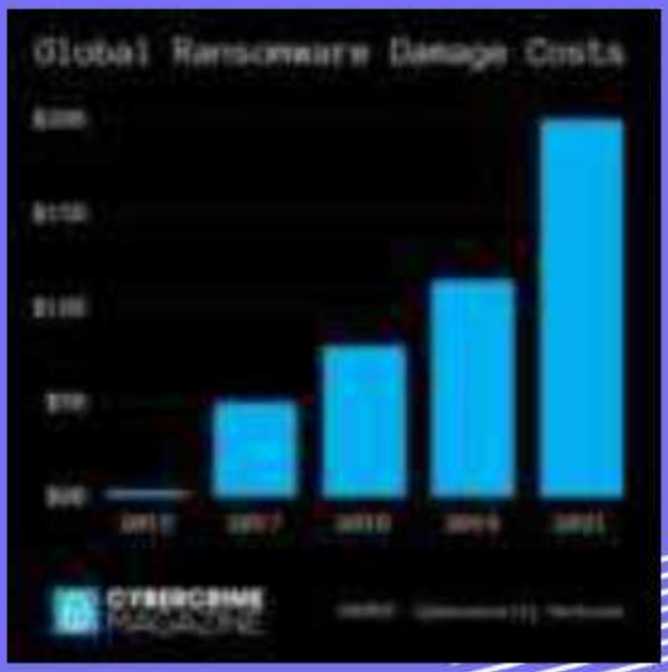
PenTest stands for Penetration Test: A Simulated Cyber Attack to assess the system's security. During PenTesting assessment, ethical hackers develop simulated systems or processes to try to attack the technology applications, technology infrastructure and identify vulnerabilities. These security flaws must be addressed to ensure no organization or individuals, for personal gains, try to exploit such vulnerabilities that end up costing the organization. Pentesting is a component of a comprehensive web application security strategy.



INSUREDMINE'S BUSINESS CASE TO INVEST IN PENTEST

High-profile security breaches continue to be a huge concern for organizations. In 2022 ransomware is expected to cost businesses over $20 billion. Cybersecurity Ventures predicts that there will be a ransomware attack on businesses every 11 seconds by 2021-2022. As we know the cost of ransomware damages are not limited to ransom payouts but also around business reputation, business continuity and much more. This trend puts an increasing number of businesses in jeopardy. Malicious hackers are coming up with new and sophisticated forms of hacking, increasing software security vulnerability.

Having anti-virus software and a firewall is no longer sufficient to keep your company's data secure. A modern business that deals with huge client data requires a sophisticated approach to security and due diligence. Therefore, a cyber security defense test in the form of a PenTest is highly effective to find out security loopholes which can be further fully proofed with effective defense mechanisms and remediation strategies.



6 REASONS WHY INSUREDMINE DECIDED TO INVEST IN PENTEST?

Crucial Data: Full-Proof Security

InsuredMine is extremely concerned about the organization's data health and security. We understand that we deal with the vital data of our clients. These are not only our clients' sales data but also the personal information of the end-users—the insureds. So, there is no other choice than to be fully proofed when it comes to data security.

1. Reduce Network Downtime

The insurance business is all about quick response and instant service so that no lead slips out of your sales pipeline.

Downtime on the network disrupts the workflow and results in financial losses. A cyber-attack slows down the system, and thus, your workflow gets slowed down too. This results in a drop in the quick response and service that your clients expect from you, which further hampers the business. Penetration testing assists in keeping your CRM software in good working order by resolving issues that may cause network downtime.

2. Reduce Remediation Costs

Data breach costs increased from USD 3.86 million to USD 4.24 million in 2021, the highest average total cost in the 17-year history of this report. - The Cost of Data Breach Report by IBM

Recovery from a security breach can cost your company thousands, if not millions, of dollars in expenses such as customer protection programs, regulatory fines, and lost business operations. According to a recent study by IBM, the average global cost of a data breach in 2021 was $4.24 million, which is 10 percent higher than the previous year's result. As a result, getting everything back on track and running will necessitate significant investments, advanced security measures, and weeks of recovery.

3. Prevention is Better than Cure

Keeping the cost of curing cyber-attacks in mind, InsuredMine chose to follow the prevention route. That is why we have opted for a penetration test as a proactive solution to identify the most vulnerable areas of our IT system. This way, we ensure to safeguard ourselves from financial and reputational losses.

4. Creates a secure environment within our organization

The more we stay secure, the more we gain the trust of our clients.

One of the major reasons agents trust us and do business with us is because they feel their data is in safe hands. And YES, IT IS FOR SURE! We follow all the necessary procedures and make the necessary investments to create a more secure environment within our organization.

5. Develop Effective Security Measures

The results of a PenTest helps us assess the current security level of our IT system. The insightful information helps us identify the security gaps and reveals the potential impact on the system's functioning and performance. The list of recommendations for timely remediation assists us in developing a dependable information security system.

6. Maintain the Company's Image and Customer Loyalty

Security breaches may compromise your sensitive data, resulting in the loss of trusted customers and severe reputational harm. Penetration testing can assist you in avoiding costly security breaches that jeopardize your organization's reputation and customer loyalty.

A pen test provides even more detailed information about vulnerabilities and potential breach points in your IT infrastructure.

THE PENTEST STAGES THAT WERE FOLLOWED IN INSUREDMINE

PLANNING & INVESTIGATION

Test goals are set and intelligence data is gathered to target the potential vulnerabilities.

SCANNING

Evaluating the reaction of our CRM application to various intrusion attempts. Both static and dynamic analyses have been carried out.

OBTAINING UNAUTHORIZED ENTRY

Dummy web attacks are staged to identify vulnerabilities and understand the damage that may happen.

KEEPING ACCESS

The goal of this stage is to determine whether the vulnerability can be used to maintain a persistent presence and if it can gain in-depth access to steal an organization's most sensitive data.

ANALYSIS & CORRECTIVE MEASURES

Penetration test results are analyzed and the Web Application Firewall is configured to patch security flaws and protect against future attacks.

METHODS THAT INSUREDMINE FOLLOWED DURING PENETRATION TESTING

01. External Evaluation

During external penetration tests, our company's internet-visible assets, such as the web application, the company website, and email and domain name servers (DNS), have been tested. The goal is to gain access to and extract useful information.

02. Internal Evaluation

During the internal test, a phishing attack test was carried out to test the company's firewall security.

03. Blind Test

A blind test was followed out to get a real-time view of how an actual application assault would occur.

04. Double-blind Evaluation

A simulation attack test has been carried out without any prior knowledge to check the performance of our security.

05. Specific Testing

The PenTester and the security personnel of our organization collaborated and performed a security test. Excellent training was further provided to our security team with real-time feedback from the perspective of a hacker.

PENTEST: OUR DATA SECURITY AUDIT

InsuredMine focuses on security as we know it is of the utmost priority to safeguard our clients' sensitive data. The PenTest helped us to ensure the safety and security of our clients' data. We value time as time is money in the insurance business. We ensure 24/7 communication and network availability that keeps you connected with your clients always. We help you with uninterrupted access to resources at any time to ensure that your business operations are always up and running. We are ready to invest to keep your data secure. Remember, your faith is our fuel!

CONNECT WITH US

+1 469-616-1821

support@insuredmine.com

200 Chisholm Pl, Suite 103
Plano, TX 75075

INSUREDMINE

Copyright © 2022 InsuredMine, All Rights Reserved.