ReconwithMe

WHITEPAPER

Abstract

The application industry is growing at a rapid rate. Web and Mobile applications are the go-to tools for people, businesses and organizations. With the increasing growth in the use of these applications, there has been growth in cyber attacks as well. The results of these attacks have incurred billions in financial losses and incalculable losses in brand and customer trust. In 2020, financial loss due to cyber attacks reached a record high $ 1 trillion, average cost of a data breach reached $3.86 million and 60% small businesses were found to shut down business in six months once they suffer from a cyber attack. Defending against cyber attacks is challenging and complex, but not as complex as people think it to be. In fact, 80% of cyber attacks can be prevented via vulnerability management, patching, and proper configurations and another 20% can be prevented via implementing strong security policies and measures against social engineering attacks. The purpose of ReconwithMe is to help businesses prevent cyber-attacks through vulnerability management, patching, secure configurations, adoption of strong security policies and measures against social engineering attacks as per business needs.

Cyber Security In 2021

Cyber Security in the decades from 1980 to 2010 was mostly about antiviruses, malware, and firewalls. Attackers would inject malware into the host's system and steal credentials and other sensitive information or take the system down. To defend, entities would install antivirus and firewalls in their system.

However, the past decade has seen the cybersecurity domain change dramatically. With everything moving to the cloud, as data moved from devices to servers, attackers began developing new techniques that would allow them to exploit servers and databases. This has led to the invention of new attack vectors every day. Attack vectors that are evolving with time. One particular solution is not enough to prevent cyber attacks as attackers seem to find new ways of exploiting systems. The need for a proactive approach to defend against cyberattacks has been felt. The proactive approach that we're talking about here is not a single solution but rather a combination of multiple solutions such as vulnerability management and patching, secure configurations, strong security policies, and measures against social engineering attacks.

Vulnerability Management

Finding Vulnerabilities

Vulnerability management is the process of identifying and patching security vulnerabilities (also called security bugs) present in an application. A study from Ponemon Institute for ServiceNow found out that 60% of cyber-attacks happen because of unpatched vulnerabilities. It simply means that you can decrease the chances of happening a cyber attack upto 60% by proactively finding and patching vulnerabilities present in an application. Here's how one can manage vulnerabilities proactively.

1. Source Code Review - Finding security bugs in lines of codes and patching them; is also called white-box testing).
2. Vulnerability Scanners - Using vulnerability scanners such as ReconwithMe to find security bugs before an application is launched. Vulnerability scanners should also be used on a regular basis (weekly or monthly) to proactively detect vulnerabilities.
3. Manual Testing - Performing VAPT and Red Teaming using security researchers (hackers) to find vulnerabilities from hacker's perspective.
4. Bug Bounty Programs - Launching public/private bug bounty programs to allow an army of hackers to find security issues in your system and report it for fixing and reward them rightly. The idea of bug bounty programs is to discourage any wrongdoings.

Managing Vulnerabilities

Managing vulnerabilities is the process of sorting vulnerabilities on the basis of severity(risks) and fixing them according to priority. The equation of managing vulnerabilities is simple; bugs with high severity (high risk) should be patched first. Bug trackers can be used to manage and fix vulnerabilities according to severity.

Patching

Patching is the process of fixing identified vulnerabilities. Patching requires specific expertise; a developer with knowledge about security or a security researcher with programming skills. Often, organizations have a triage team to resolve vulnerabilities.

Secure Configurations

Any integrations such as DNS, Server, Firewall, or Third Party (Zira, Slack, Stripe etc) for the application must be configured securely. Secure configurations of web applications can be done in the following way.

- Configure HTTP Headers - Test for access control bypass, XST vulnerabilities, HTTP method overriding techniques and review the HSTS header and its validity.
- Configure Application Platform - Ensure that defaults and known files have been removed; Validate that no debugging code or extensions are left in the production environments; Review the logging mechanisms set in place for the application.
- Configure Network Infrastructure - Review the applications' configurations set across the network and validate that they are not vulnerable; Validate that used frameworks and systems are secure and not susceptible to known vulnerabilities due to unmaintained software or default settings and credentials.
- Configure File Extension for sensitive information - Dirbust sensitive file extensions, or extensions that might contain raw data (e.g. scripts, raw data, credentials, etc.); Validate that no system framework bypasses exist on the rules set.
- Configure RIA Cross Domain Policy - Review and validate the policy files.
- Configure File Permission - Review and identify any rogue file permissions.
- Configure SubDomains - Enumerate all possible domains (previous and current); Identify forgotten or misconfigured domains.
- Configure Cloud Storage - Assess that the access control configuration for the storage services is properly in place.

Security Architecture

Designing a security architecture simply means making sure that the flow of data and information between various components (Devices, People, Processes) within a business or third party (Consultants, Vendors, Partners) is secure. Security Architecture helps strike a balance between devices (server, computers, laptop, wifi, IOTs), people (owners, employees, users), and processes, ultimately reducing the risks of cyberattacks.

Security Policy

While security architecture helps streamline the flow of data and information in a secure manner, security policy helps define control measures (who controls what) to make sure that stakeholders (owner, employees, users, processes) have access to data and information that are essential. For example, a CTO or a project manager in an organization can have access to the server, but, it's not necessary for a marketing officer to have such access. If a marketing officer has such access, then it increases the risk of a cyber attack. Thus, a strong security policy that clearly defines control of information in an organization should be in place in order to prevent cyber attacks.

Social Engineering

Social Engineering is the art of manipulating people to get access to sensitive information. Phishing, Vishing, Smishing, Honey Trapping are some of the examples of social engineering. Non-technical workforce are highly vulnerable to social engineering attacks. Measures such as organizing social engineering workshops, can be taken to educate and aware non-technical workforce about different forms of social engineering attacks.

Simplifying Web Application Security

ReconwithMe's vision is to simplify application security by introducing effective and efficient measures of preventing cyber-attacks for both individuals and businesses. You might be an individual doing business from your website, you might be an owner or CISO of a small company with few thousands in revenue or you might be an owner or CISO of a big company with millions in revenue. ReconwithMe will help you identify and implement the right application security solution.

ReconwithMe's 80-19 Web Application Security Framework

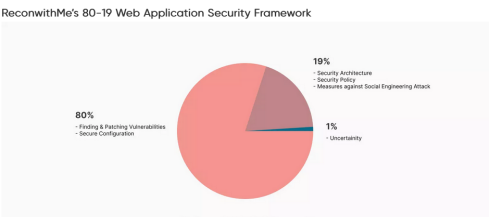

Fig 1 : ReconwithMe's 80-19 Web Application Security Framework

Our experience as cybersecurity professionals providing various cybersecurity solutions for years has taught us that preventing cyber attacks is definitely challenging but not complex. We've come to a conclusion that 80% of cyber attacks can be prevented via vulnerability management, patching, secure configurations, and another 19% can be prevented via implementing strong security policies and measures against social engineering attacks (1% for the odds that anything can happen). This is what we're calling the "ReconwithMe's 80-19 Cyber Security Framework."

The 80-19 equation;

Finding Vulnerabilities + Patching + Secure Configurations = 80% decrease in chances of a cyber attack.

Security Architecture + Security Policy + Measures against Social Engineering Attack = 19% decrease in chances of a cyber attack.

The first thing a hacker will do to exploit your system is by trying to find security loopholes which we call bugs or vulnerabilities. By patching vulnerabilities present in an application, one can reduce the risk of cyber attacks up to 60%.

How to find and patch vulnerabilities?

- Recruit a security team or outsource to a trusted third party.
- Use Automated tools such as ReconwithMe and perform Vulnerability Assessment and Penetration Testing on a regular basis.
- Launch private/public vulnerability disclosure programs
- Manage vulnerabilities according to priority (from high risk to low-risk vulnerabilities)
- Apply fixes with the help of security experts.
- Re-test to confirm fixes.

Finding and Patching Vulnerabilities using ReconwithMe

One can use ReconwithMe to find and manage vulnerabilities. Using ReconwithMe's automated scanning feature you can detect upto 80% of vulnerabilities that exist in your web application. If you want to dig deep and find more vulnerabilities you can request for a manual penetration testing and even launch a bug bounty program in coordination with our security team. Once you complete a scan, you'll see a list of vulnerabilities in the Bug Tracker that will help you to manage bugs (Sort out and fix according to priority). You can also manually add vulnerabilities using the "Add" button in the bug tracker. If you run into problem fixing a bug, you can ask for help from our triage team.

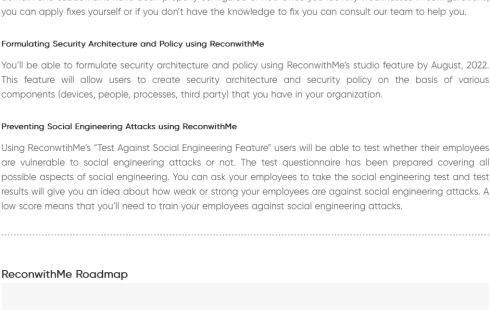

Fig 2: Vulnerability Management Cycle.

Always remember that vulnerability management and patching is not a one time thing, it is a continuous process. Once vulnerabilities are found and fixed, the next step is to make your configurations secure. This will decrease the chances of cyber-attack by another 20%.

Secure Configurations using ReconwithMe

ReconwithMe's scanner doesn't only scan for vulnerabilities. It also looks for security misconfigurations. It will check if your HTTP headers and policies are in place or not, if http is properly redirected to https or not and if domain and subdomains have been properly configured or not. Once you identify weaknesses in configurations, you can apply fixes yourself or if you don't have the knowledge to fix you can consult our team to help you.

Formulating Security Architecture and Policy using ReconwithMe

You'll be able to formulate security architecture and policy using ReconwithMe's studio feature by August, 2022. This feature will allow users to create security architecture and security policy on the basis of various components (devices, people, processes, third party) that you have in your organization.

Preventing Social Engineering Attacks using ReconwithMe

Using ReconwithMe's "Test Against Social Engineering Feature" users will be able to test whether their employees are vulnerable to social engineering attacks or not. The test questionnaire has been prepared covering all possible aspects of social engineering. You can ask your employees to take the social engineering test and test results will give you an idea about how weak or strong your employees are against social engineering attacks. A low score means that you'll need to train your employees against social engineering attacks.

ReconwithMe Roadmap

Fig 3: ReconwithMe Roadmap

References

1. https://www.mcafee.com/enterprise/en-us/assets/reports/rp-hidden-costs-of-cybercrime.pdf
2. https://www.ibm.com/security/data-breach
3. https://staysafeonline.org/press-release/national-cyber-security-alliance-statement-regarding-incorrect-small-business-statistic/
4. https://www.ponemon.org/local/upload/file/BMC%20Consolidated%20Report%20Final.pdf
5. https://owasp.org/www-project-web-security-testing-guide/latest/4-Web_Application_Security_Testing/02-Configuration_and_Deployment_Management_Testing/README