BANK PASARGAD®

Promoting Cyber Security

ABSTRACT

Cyber security has become the integral part of any organization delivering content over the web. Bank's while complying with the utmost security principles also need to make sure that content is delivered to their users swiftly. As per the most recent study by Accenture, 85 major cyber-attacks (on average) were launched on each of the 275 bank's that were interviewed in the last year. Bank Pasargad in collaboration with our in-house banking solution and technology provider, Dotin have deployed a CDN system which ensures the high performance of our content distribution and the safety and security of the content at the same time. In addition to the CDN system, Dotin is providing Bank Pasargad with the latest tools and services in Cybersecurity including Threat Hunting, EDR, PAM, SOC, PEN Test, EMS, GRC and Red Team.

Bank Pasargad in collaboration with Dotin has adopted a hollistic strategy for cyber security for the whole organization and has defined a Cyber Security *Framwork*. This comprehensive frame work defines the best practices that are to be implemented currenntly and enhanced over the years with the evolving needs of the bank and the dynamics of the market where the bank operates.

The framework consists of the following security domains shown in **figure 1.** Each domain has been explained breifly and each domain comprises of a subset of policies and tools that can be implemented as part of the Cyber Security *Framework*. An importan aspect taken into consideration while

implementing a Cyber Security policy is the *maturity level* of the organization and its *risk management policy*. Bank Pasargad invested a lot of time and resources on defining the *Cyber Security maturity level* and the *Risk Management* policies as a part of defining their Cyber Securrity *framework* which consist of a to-do list for the present and the future. The complete *framework* can be apliied to the 4 Ps that are involved in Cybersecurity of any organization namely *People, Place, Processes and products*.

Figure 1: The BPI (Bank Pasargad Iran) security Frame Work

Some of the major tools and solutions used under the Cyber Security frramework have been discussed in detail in this document.

Table of Contents

Bank Pasargad

Bank Pasargad, the winner of 6 times bank of the year award by 'the banker', 5 times winner of the best Islamic bank award by 'the banker', and also 3 times straight winner of the Euro money award since 2015 has been promoting innovation throughout its 11 year Journey since its incorporation back in 2006.

Bank Pasargad is a very technology oriented bank with its in house technology provided by one of our subsidiary Dotin. Dotin provides the bank with the latest and the greatest tools for banking and payments and is responsible for ensuring the cyber security in addition to setting up the required network for effective communications between the branches, data centres and all the customer touch points. More than 96% of all Bank Pasargad transactions take place outside of the branches making Bank Pasargad one of the highest digital banks in Iran. The fact that roughly half a million transactions of bank Pasargad are being conducted on the internet, this makes the bank even more prone to cyber-attacks.

Bank Pasargad has been a pioneer in launching many innovative ideas in the Iran, from banking via USSD, to a social banking platform, digital financial literacy programs, green banking to being the first bank to launch CDN in Iran this year.

Dotin

Dotin is a leading provider of SOA-based multi-channel software products for banks and financial services institutions. Dotin has vast experience in implementing successful solutions for some of the biggest banks in Iran. We strive to lead in the development of the industry's most advanced financial technologies. Through our solutions and services, we translate these advanced technologies into value for our customers. Dotin has successfully designed and implemented a total suite of banking solutions to fulfill the needs of banks and financial institutions around the world. Providing comprehensive end to end front office, back office, and middleware to the banking and payments sector,

Dotin works continuously on modern developments to create long term benefits for its clients.

Content Delivery Network (CDN)

The most important role of a Content Distribution Network (CDN) is to deliver online content from the closest possible point to the user. This makes a website or any online content to load faster, and at a higher quality, thus enhancing the user's experience. Our latest cloud security allows us to safely distribute content by simply defining security rules in a cloud environment. In addition the Cloud firewall makes it possible to block access to a specific group of users

Our DDoS Protection solution help's protect our websites and online services against DDoS attacks without any need to change their hosts, their network architecture, or their code.

The latest CDN solution deployed by Dotin for Bank Pasargad uses advanced Anycast architecture and its Global Server Load Balancing (GSLB) technology to fend off UDP, TCP, layer 3 or layer 4 ICMP, layer 7, or DNS server attacks.

Web Application Firewall (WAF) is the system tasked with preventing traditional and advanced cyber-attacks. This system helps neutralizes most of the common and advanced web attacks without the need for technical know-how.

In line with the stringent security polices of the Bank, a private cloud and dedicated CDN seemed as the best option to maximize the cyber security of the bank. Usually, most companies that provide CDN services use their own public infrastructure in order to offer services to the banks. In the case of Bank Pasargad, Dotin has provided the complete CDN solution on premises of Bank Pasargad. Dotin's task was daunting since this was the first time a CDN was being implemented in Iran. The project was different from any CDN project that we know of around the world since in case of Bank Pasargad, Dotin had to deliver a dedicated infrastructure fully functional and operational under the

supervision and management of the bank. After the implementation and go-live, the vendor (Dotin) was to have no access to any bank information anymore.

There were two main goals of Bank Pasargad for implanting CDN. The first goal was increasing the performance and the quality of the web based services in the banks. Dotin offered a range of edge servers to Bank Pasargad as part of the CDN. The users are connected to the closest server to their geographical location and as a result, they experience a faster and higher quality of usage. The service reduced the average load time of Bank Pasargad's online services by 40 to 70%. A page that would load in 1 second before implementing CDN now loads between 0.6 to 0.3 seconds.

The second goal was increasing the security of these services and the management of security of services in an integrated form. Since the implementation many attacks, including a DDos attack with the volume of 200 Gb/ps have been fended off. Furthermore, thousands of cyber-attacks to banking web services were fend off, using WAF (Web Application firewall). Several cyber attacks were blocked and among them the most recent ones was a DDoS attack that was blocked.

Cyber threat hunting

A threat hunting solution implemented by Dotin provides proactive security search through networks, endpoints, and datasets to hunt malicious, suspicious, or risky activities that have evaded detection by existing tools. Through Threat hunting an experienced cybersecurity analyst proactively uses manual or machine-based techniques to identify security incidents or threats that currently deployed automated detection methods did not catch. Our expoert analysts know how to coax their toolsets into finding the most dangerous threats. They have require ample knowledge of different types of malware, exploits and network protocols to navigate the large volume of data consisting of logs, metadata and packet capture (PCAP) data.

Endpoint detection and response (EDR)

Dotin’s EDR solution is an integrated endpoint security solution that combines real-time continuous monitoring and collection of endpoint data with rules-based automated response and analysis capabilities.

The primary functions being performned by the EDR security system are:

1. Monitor and collect activity data from endpoints that could indicate a threat
2. Analyze this data to identify threat patterns
3. Automatically respond to identified threats to remove or contain them, and notify security personnel
4. Forensics and analysis tools to research identified threats and search for suspicious activities

Privileged Access Management (PAM)

Bank has implemenetd an in-house information security (infosec) mechanism that safeguards identities with special access or capabilities beyond regular users. Our PAM works through a combination of people, processes, and technology. Privileged access allows organizations to secure their infrastructure and applications, run business efficiently and maintain the confidentiality of sensitive data and critical infrastructure. We have designed our PAM solution to provide privileged access to both human users as well as non-human users such as applications and machine identities.

Security Operation Center (SOC)

We have a Security Operation Center which provides a centralized function within an organization employing people, processes, and technology to continuously monitor and improve an organization's security posture while preventing, detecting, analyzing, and responding to cybersecurity incidents.

Our SOC acts like the hub or central command post, taking in telemetry from the bank’s IT infrastructure, including networks, devices, appliances, and information stores, wherever those assets reside. Our SOC is the correlation point for every event logged within the organization that is being monitored.

For each of these events, the SOC decides how they will be managed and acted upon.

PENETRATION TESTING

Our team perform various kinds of Pen testing including ethical hacking. We describe an intentional launching of simulated cyberattacks by penetration testers using strategies and tools designed to access or exploit computer systems, networks, websites, and applications. The main objective of pen testing is to identify exploitable issues so that effective security controls can be implemented, however bank Pasargad's team uses penetration testing techniques, along with specialized testing tools, to test the robustness of our organization's security policies, its regulatory compliance, its employees' security awareness, and the organization's ability to identify and respond to security issues and incidents such as unauthorized access, as they occur.

Enterprise Mobility + Security (EMS)

Bank Pasargad has implemented an enterprise grade IT solutions for mobile device and identity management, data protection and threat detection; all combined into one package. With each and every employee bringing a device of their own, EMS is cost effective and enables IT teams to provide conditional access to devices, apps and data with cross-platform functionality across iOS, Android and Windows. We enhanced our security through policy and encryption.

Governance, Risk, Compliance (GRC)

Our set of tools and services mentioned above empowers the bank to pursue an integrated approach to GRC and ensure collaboration between risk, compliance, audit, cybersecurity, and sustainability teams. This highly collaborative approach enables all different departments to better identify, assess, manage, and mitigate strategic risks, operational and enterprise risks, IT and cyber risks, third-party risks, compliance risks, and environmental, social, and governance (ESG) risks. Designed with advanced analytics and AI capabilities at its core, our solutions deliver GRC best practices.

Red Team Excercise

Dotin performs red team excercises for bank Pasargad regularly. In a red team/blue team exercise, the **red team** is made up of offensive security experts who try to attack the bank's cybersecurity defenses. The **blue team** defends against and responds to the red team attack. In a red team/blue team cybersecurity simulation, the red team acts as an adversary, attempting to identify and exploit potential weaknesses within the organization's cyber defenses using sophisticated attack techniques. These offensive teams typically consist of highly experienced security professionals or independent ethical hackers who focus on penetration testing by imitating real-world attack techniques and methods.

Conclusion

The usefulness of the above mentioned tools from CDN all the way to Red Team excercise can be determined by the time and cost it saved the bank by giving faster services to its online users and deterring cyber threats that were launched against the bank. As a result, the users' trust is increased regarding the bank security. In addition, using CDN for banks, increases the quality of web services and enhances the quality of user experience which can be considered a great advantage in the market.

Bank Pasargad has been the trendsetter in providing value added banking and payment solutions and services to the masses in Iran. The bank has transformed the way people bank in Iran by conducting more than 96% of its transactions out of the branches. We have transformed the mind set of people by conducting training sessions in branches, as well as outside the branches via internet and mobile to increase the financial literacy among the people of Iran. We are active in corporate social responsibility acts of enabling green banking, setting up public libraries, contributing to the development of education in rural areas, setting up a University (Khatam) and sponsoring sports team including the national wresting and football team.

We have set out to transform the cyber security and web performance through this first ever CDN project in Iran. A unified cloud security system is considered an important competitive value for any bank. One of the biggest challenges for the banks today is dealing with DDos attacks. Our systems have the potential to fend off extensive Cyber attacks and hence decreases the chance of down times of online services in times of attack. Also, the cloud WAF (Web Application Firewall), protects the system against cyber-attacks that lead to anomalies in the service or data leakage.

Bank Pasargad has raised the standards of cyber security in Iran and has in turn forced other banks to rethink their cyber security strategy. Six other banks have approached Dotin and are discussing replicating the services of CDN, Threat Hunting, EDR, PAM, SOC, PEN Test, EMS, GRC, Red Team and private cloud in their respective banks.