CLOUDFLARE®

Checking the Box made Easy

Meet the FFIEC cyber-crime requirements for community and regional banks

1 888 99 FLARE | enterprise@cloudflare.com | www.cloudflare.com

Executive Summary

Cyber-attacks constitute an entirely new threat vector, which is especially concerning and troublesome to banks. While there are many examples of recent high profile cyber-attacks against banks, attacks occur against any type of organization, large or small. Mounting sophisticated and powerful cyber-attacks is now easily accessible to everybody and therefore it cannot surprise that these attacks are getting more and more frequent and powerful. Traditional on-premises hardware based solutions are easily overwhelmed and proved ineffective.

As a result, the FFIEC requires banks to take a comprehensive approach to maintain the security and resilience of the technology infrastructure including the establishment of a robust cybersecurity framework. However, the regulatory system reflects the processes of the largest banks and therefore community and regional banks face an overproportional cost burden to meet the requirements.

Cloudflare can help to protect critical financial systems against cyber-attacks while achieving the regulatory compliance requirements set forth by the FFIEC, by providing:

- Layer 3 and layer 4 DDoS protection through anycast-based network resilience
- Layer 7 DDoS protection through rate limiting and an IP Reputation Database
- Layer 7 application vulnerability attack protection through a Web Application Firewall
- Implementation of the Domain Name System Security Extensions (DNSSEC)

Setting up Cloudflare to get access to those capabilities is a major step forward for community and regional banks to achieve FFIEC cyber-crime compliance.

Banks, large and small, are the new target for cyber-attacks

The recent cyber-attacks against high profile banks grasp the attention and make the news headlines. However, attacks against community and regional banks occur as well but they simply don't get highlighted to the same extend. Community and regional banks can learn from the well-publicized examples, some of them are listed below, to better understand the threats in order to put measures in place to get prepared.

On May 4th 2016 hackers published a list of 160 banks as targets for cyber assault including some big names such as the US Federal Reserve Bank, the IMF, the World Bank, the New York Stock Exchange and the Bank of England. Within only a few days, the sites of more than 10 banks were brought offline by DDOS attacks, in a sophisticated effort that lasted 30 days.[1]

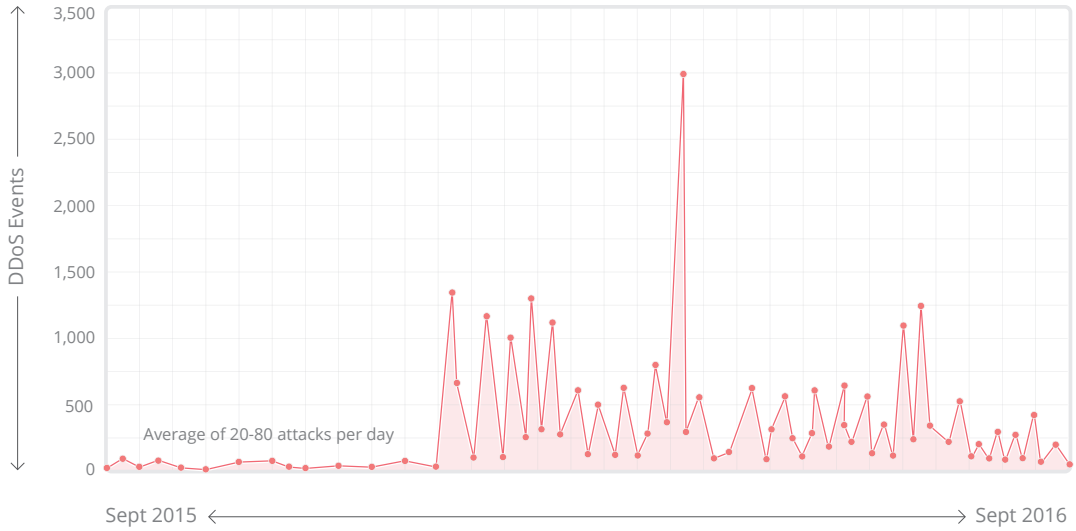
In another recent type of a cyber-attack hackers used fraudulent Swift messaging to trick the Federal Reserve Bank of New York to send funds to Bangladesh's central bank. $81M in foreign reserves were stolen and the transfer of a stunning $850M was only prevented by pure luck: the hackers misspelled the name of one of the recipients. Unfortunately, this type of attack is popular as well: other examples include Ecuador's Banco del Austro, which lost ~$12M, and Vietnam's Tien Phong Commercial Joint Stock Exchange, which was also targeted.

While successful cyber attacks against high profile banks capture the headline news, attackers target any size of organization

Other types of cyber-attacks involve breaches in secure data. In 2014 the networks of JPMorgan Chase & Co. were penetrated and information on millions of customers were compromised. Another recent example is the breach of Qatar National Bank (QNB), where 1.4 GB of sensitive information was leaked.[2]

Cloudflare, which sees about 11 million HTTP requests per second, can filter and accurately measure cyber-attacks. Over the last year Cloudflare observed the number and intensity of attacks increasing, with up to 1,400 DDoS (Distributed Denial-of-Service) events per day, an aggregated 400Gbps of incoming traffic and 200M packets per second.

Daily L3 DDoS Attacks



Attacks are often not one-off events and victims are typically targeted multiple times in a year. According to Cloudflare's experience, anybody—large and small organizations alike—can be targeted. Even though many jurisdictions have laws under which DDoS attacks are illegal, there are DDoS-as-a-Service providers offering subscriptions, some starting as low as at $5-$10/month, which can be used to mount sophisticated and powerful cyber-attacks.

In this arms-to-arms race, even sophisticated on-premises hardware solutions are now ineffective as they can easily be overwhelmed by DDoS attacks. Even the biggest available hardware solutions can no longer match the size of larger DDoS attacks. In addition, hardware based solutions are often cost prohibitive, only scale through clustering and require highly trained specialized administrators or outside assistance. Lastly, new larger attack patterns require fail over to even more expensive hybrid-cloud based solutions.

Guidance and regulatory requirements by the FFIEC to mitigate cyber attacks[3]

The U.S. Executive Branch is responding to the new cyber-attack threat vectors. On 7/26/2016, President Obama released the Presidential Policy Directive-41. This directive states that while cyber incidents are a fact of contemporary life, significant cyber incidents are occurring with increasing frequency, impacting public and private infrastructure located in the United States and abroad. The policy directive sets forth principles governing the Federal Government's response to any cyber incident, whether involving government or private sector entities.[4]

The White House
Office of the Press Secretary

For Immediate Release July 26, 2016

Presidential Policy Directive -- United States Cyber Incident Coordination

July 26, 2016

PRESIDENTIAL POLICY DIRECTIVE/PPD-41

SUBJECT: United States Cyber Incident Coordination

Financial institutions are regulated by the Federal Financial Institutions Examination Council (FFIEC), which also has strongly raised awareness on cyber risks. According to the FFIEC, cyber threats may originate from nation-states, terrorist, criminal enterprises or insiders, and their impact might include lost financial assets, stolen customer information, stolen intellectual property, business disruption and damaged reputation. The FFIEC states:

> An institution should take a comprehensive approach to maintain the security and resilience of its technology infrastructure including the establishment of a robust cybersecurity framework. The framework should incorporate processes to identify, prevent, detect, respond to, and recover from technology-based attacks.
>
> - FFIEC, Cybersecurity and Resilience Against Cyber-Attacks[5]

Furthermore, the FFIEC is empowered to prescribe uniform principles, standards, and report forms for the federal examination of financial institutions and to make recommendations to promote uniformity in the supervision of financial institutions. Banks are required to establish an effective audit program to evaluate risk management practices, internal control systems and compliance with corporate policies concerning IT-related risks, with audits ordinarily being scheduled once a year.

While the U.S. banking industry has been strongly consolidating over the last three decades, the remaining smaller banks are subject to the same regulatory system as the few large ones. Even though the plans to implement the regulatory requirements should be adapted to the size and complexity of the institution, the regulatory system itself reflects the processes of the largest banks. Therefore, community banks face an overproportional cost burden to meet compliance and it comes as no surprise that surveys indicate regulatory burden as a continuing concern and as the number one reason for planned exists of banks.[6]

The 6,524 U.S. community banks, which together hold 15% of the assets, are subject to the same regulatory system as the top 4 U.S. banks, which hold 45% of the assets.[7]

The FFIEC provides several Information Technology Examination Handbooks (IT Handbooks) to identify areas of greatest IT risk exposure to the institution and to promote the confidentiality, integrity and availability of information systems. Relevant IT handbooks include:

- **Business Continuity Planning:** Provides guidance to ensure the availability of critical financial services and on the importance of business continuity planning, which establishes the basis for financial institutions to recover, resume and maintain all critical business functions when operations have been disrupted unexpectedly
- **E-banking:** Provides guidance to identify and control the risks associated with electronic banking. The handbook distinguishes between risks when reviewing informational websites and transactional websites. Transactional e-banking services expose the bank to higher risks
- **Information Security:** Provides guidance to assess the risks to a financial institution's information system, and promotes the commonly accepted objectives of confidentiality, integrity, and availability of information
- **Retail Payment and Wholesale Payment System:** Provides guidance on risks related to retail payment systems and transmitting large-value payments (e.g. using the Swift network for international funds transfer). While those books cover important risks such as preventing financial loss, for this discussion the focus is on implementing measures to mitigate or limit operational risks associated with authentication and encryption techniques, as well as preventing unauthorized access to information in transit

Essential technologies to protect against cyber-attacks and to achieve FFIEC compliance

Cloudflare operates one of the world's largest networks that powers more than 10 trillion requests per month, including requests for ~10% of the Fortune 1000. Through this network, Cloudflare can help banks to protect critical financial services against cyber-attacks and to achieve FFIEC compliance. Setting up Cloudflare does not require any additional hardware, installing any software, or changing any line of code, making it much easier to achieve compliance. Cloudflare's key capabilities include:

Layer 3 and layer 4 DDoS protection: Anycast network resilience with automatic learning platform

Cloudflare's advanced DDoS protection, provisioned as a service at the network edge, matches the sophistication and scale of the threats and can be used to mitigate DDoS attacks of all forms and sizes. Cloudflare prevented many of the largest DDoS attacks in history including attacks over 400Gbps in size.

Layer 3 and layer 4 DDoS attacks are usually volumetric attacks such as DDoS amplification, DDoS flood and DDoS SYN flood attacks. While those attacks can overwhelm a typical unicast based network, Cloudflare's Anycast based network inherently increases the surface by spreading the attack traffic to each of the more than 100 Cloudflare datacenters and to a diverse set of high bandwidth interconnections with other networks, to simply absorb the attack traffic. In addition, Cloudflare provides an automatic learning platform, where network traffic is analyzed in real time to identify anomalous or malicious requests. Once a new attack is identified, Cloudflare automatically starts to block that attack type for both the particular website and the entire community.

As Cloudflare continues to grow its network and its community, it will get harder and harder to launch an effective DDoS attack against any of Cloudflare's users.

Layer 7 DDoS protection: Rate Limiting with IP Reputation Database

Like Layer 3 and 4 volumetric attacks, Layer 7 Denial of Service attacks use a high volume of requests to prevent real users from accessing a website. In layer 7 Denial of Service attacks the requests are similar to the pattern of normal non-malicious traffic, and thus they are difficult to protect against.

Cloudflare's Traffic Control—currently available through an Early Access Program—tracks the number of requests coming to a site from each IP address and identifies sites that make too many requests per minute. Once a suspicious IP address is identified, traffic from this IP address is presented with an interstitial page for about 5 seconds to perform a series of mathematical challenges. If the request fails this challenge, Traffic Protector downgrades that IP's reputation and traffic from this address will be shown a CAPTCHA page with every access attempt.

When Cloudflare identifies an IP address that appears to be making malicious requests it is stored in the Cloudflare IP Reputation Database. Based on a threat score a request either goes through or the request is presented with a CAPTCHA. If the CAPTCHA fails and the IP address is identified as malicious, the request is blocked at Cloudflare's edge for the entire network, benefiting the entire Cloudflare community.

Layer 7 (non-DDoS) application vulnerability attack protection: Web Application Firewall

Layer 7 application layer attacks are the most complicated and sophisticated types of attacks. By mimicking normal use of an application, they are able to get past most DDoS mitigation equipment and vulnerability protection services. Common types of attack include SQL injection and Cross-Site Scripting (XSS), which might allow attackers to access and tamper with customer or any other kind of sensitive data.

Cloudflare addresses those threats via its Web Application Firewall (WAF). The WAF implements the Open Web Application Security Project (OWASP) Core Rule Set, which specifies the most critical security risks faced by organizations. In addition Cloudflare provides out of box rules as well as custom rules created by the community/ customers. A new rule released by Cloudflare will propagate to all Cloudflare server nodes within 30 seconds and the WAF itself adds less than 1ms of latency per request, providing security without any performance tax. This way Cloudflare has been able to protect their customers against major Zero-Day vulnerabilities including the Shellshock vulnerability or the Heartbleed Bug.

Implementation of the Domain Name System Security Extensions (DNSSEC)

The Domain Name System (DNS) is one of the pillars of authority on the Internet providing the mechanism to map domain names to Internet Protocol (IP) addresses. When DNS was designed in the early 1980s there was no consideration for strong security mechanisms in the protocol, and as the network grew, DNS remained unchanged as an insecure and unauthenticated protocol.

DNSSEC are security extensions to DNS. They add protection for DNS records so that all answers from DNS can be trusted. DNSSEC ensures to DNS clients origin authentication of DNS data, authenticated denial of existence and data integrity. They protect against man-in-the-middle attacks and DNS poisoning attacks, which could allow arbitrary attacker to trick DNS, and redirect web browsers and other applications to incorrect servers allowing them to hijack traffic.

Cloudflare has implemented DNSSEC for its customers. At the core of DNSSEC is a trust chain sequence.
The beginning of the chain is the root key which is maintained and managed by the operators of the DNS root.
The records within the trust chain sequence identify either a public key or a signature of a set of resource records.
While DNSSEC is complicated, Cloudflare provides a fully managed solution to take away the complexities and make it simple for customers.

In addition to the key capabilities described above, Cloudflare supports:

- TLS 1.3 and HTTP/2 with Server Push
- Keyless SSL
- BANK domain compliance requirements

Lastly, Cloudflare's Content Delivery Network can help to improve the performance of e-banking sites and mobile apps while offering flat rate pricing, that does not change with cyber-attacks.

Note: Cloudflare has attestations for PCI DSS 3.1 as a Level 1 provider and is currently being audited to 3.2.
In addition, Cloudflare's roadmap includes obtaining certification for SSAE 16 SOC 2 Type 1 and subsequent Type 2.

Takeaways

Checking the box that your community or regional bank is protected against cyber-attacks and can achieve FFIEC regulatory compliance is made easy by signing up with Cloudflare. **The setup is very simple and usually takes less than 5 minute to get up and running.**

Check out the plans, ranging from free to enterprise at www.cloudflare.com.

References

[1] http://www.itproportal.com/2016/05/10/anonymous-op-icarus-campaign-targets-banks-worldwide/
http://www.ibtimes.co.uk/opicarus-hacker-reveals-why-anonymous-attacking-world-banks-who-next-target-1559335

[2] Bloomberg Technology, Jesse Hamilton, 7/8/2016, Bank cyber-attacks said to prompt Fed to prepare new safeguards
Bloomberg Technology, Laurence Arnold and Alan Katz, 5/23/2016, Quick take Q&A: Global Banking's message system attracts hackers
Bloomberg Technology, Arun Devnath, 3/13/2016, Bangladesh Slams 'Incompetent" central bank after hack theft

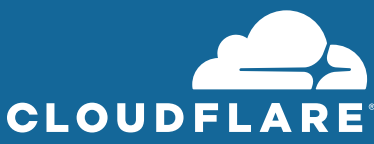
[3] http://www.ffiec.gov/about.htm

[4] https://www.whitehouse.gov/the-press-office/2016/07/26/presidential-policy-directive-united-states-cyber-incident

[5] FFIEC, Cybersecurity and Resilience Against Cyber-attacks, http://www.ffiec.gov/press/PDF/FFIECCyberSecurityBrochure.pdf

[6] CSBS, Federal Reserve and CSBS Release Findings from 2016 National Survey of Community Banks, 9/29/2016

[7] FDIC, FDIC Community Banking Study, December 2012



1 888 99 FLARE | enterprise@cloudflare.com | www.cloudflare.com