StackPath

Threat Landscape for Startups Building Web Applications

LEONARD T. MARZIGLIANO, CISSP-ISSMP

OCTOBER 2016

ABSTRACT

This report maps out the landscape of cybersecurity threats in a 'spectrum' of threat actors and examines mitigation solutions through the lens of startup companies building web applications. It then turns toward solutions for protecting and defending against these threats that can be implemented at each phase of the system development lifecycle.

Table of Contents

BACKGROUND: Adversarial Intent

Strategic Threat Types

Strategic threats are any entity that might act in an adversarial way toward the confidentiality, integrity, or availability of your organization's information or systems. The intent of an adversary can often reveal much about the origins, motivations, and expected behaviors of that adversary, and thus indicates how to enact the most effective defenses to prevent or mitigate their attacks. Strategic threats are classified into three broad types, defined by a base characteristic of their adversarial intent:

Untargeted Threats

Untargeted threats are from adversaries seeking targets of opportunity, usually based on specific technologies. An example of an untargeted threat is someone seeking only WordPress sites to attack, without regard to the organization that might be affected. Attacks of this nature are often launched in massive volumes, driving the need within organizations for automated intrusion prevention systems, behavior-based protection mechanisms, and reputation-based filtering technologies.

Targeted Threats

Targeted threats act on various motives against the technology of specific systems or organizations, either singularly or as part of a coordinated effort against a select group. These threats are less in number than untargeted threats, but carry a much higher chance of success and severity of impact.

Advanced Persistent Threats

The lethal combination of an ardently motivated, highly capable, and narrowly targeted attacker is known as an Advanced Persistent Threat. These are always critical in severity of impact. Security firms and Computer Emercency Response Team (CERT) organizations often publish profiles and reports on publicly known APT groups that detail the behavior patterns, known exploits, and other nuances of these threats.

Automated defenses help by filtering out most untargeted attacks and publicly known exploits, thus enabling greater visibility and focus on the more crucial targeted threats and APTs. This is similar to military style force protection techniques, where clearing the building perimeter of bushes and parking spaces allows for a better view and command of the action when the truly skilled bad guys show up.

The Threat Spectrum

The landscape of threats can best be assessed through common patterns of intent on the part of threat actors. This is the impetus for the Threat Spectrum:

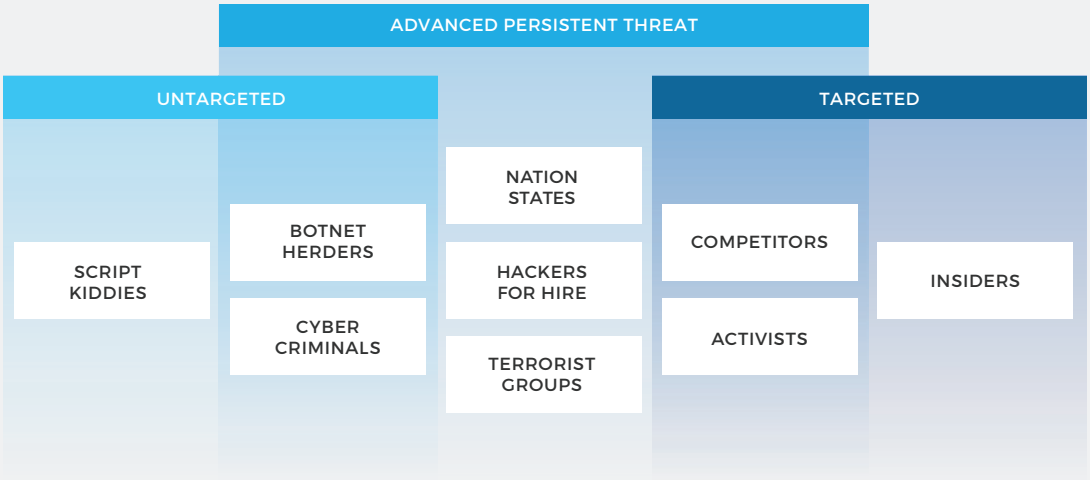

Figure 1: Composite model of the Threat Spectrum

Some threat actors commonly operate in an untargeted or targeted fashion. These are shown on the outlying sides of the Threat Spectrum model above. Others blur those lines and also sharply increase in capability and impact. These are shown in the center of the model.

An inherent migration path through this landscape exists as well: Insiders can become Competitors or Activists, Script Kiddies can grow into Botnet Herders, Cyber Criminals or Hackers for Hire, Insiders can aid or become Competitors, and Hackers for Hire can be exploited by nearly anyone, including Terrorist Groups and Nation States. This is why Hackers for Hire was selected to reside in the dead center position of the model above.

Script Kiddies

Motivation Pride | **Skill** Low/Moderate | **Likelihood** Very High | **Impact** Low

This is the most basic of threats and also the most common, yet the rate of success is still astonishingly high. Most publicly-known flaws in software are published in near-real time on commonly known message boards like BugTraq[1] and Full Disclosure[2] – then, within minutes of release, exploits published there are pasted into exploit engines like Metasploit[3]. They are then fired off at thousands of potential targets. This technique is especially dangerous for web applications as their underlying technologies are often the most commonly targeted. Fortunately, the good guys also read these forums, feeding defensive profiles into exploit prevention tools like web application firewalls.

Botnet Herders

Motivation Monetary | **Skill** Moderate/High | **Likelihood** High | **Impact** Moderate

Successful Botnet Herders are earning over $9,000 per week managing legions of exploited computers, so the incentive for them is huge. Due to the immense and adaptive capabilities they make available for rent by any other threat actor in the spectrum, botnets are a very serious threat. Thus, they are ardently maintained by their owners and heavily pursued by governments and security firms who fear the potential they have for use as powerful encryption cracking engines and other cyber weapons.

Cyber Criminals

Motivation Monetary | **Skill** High/Very High | **Likelihood** Moderate | **Impact** Extreme

Startups are often accompanied by injections of cash due to capital investments, and Sutton's Law[4] certainly applies here: Cyber criminals go where the money is and often use surprisingly diverse tools and methods to achieve their goals. The sharp increase in ransomware incidents has raised both the criticality and notoriety of cyber crime. The sudden loss of data or cash vital to any business can easily become a terminal incident for any startup.

Hackers for Hire

Motivation Monetary | **Skill** Various | **Likelihood** Moderate | **Impact** Extreme

These are highly skilled and experienced adversaries that often operate alone or in small teams. They have various skillsets and target preferences. Due to their pure financial motivations, these hackers can also appear on your threat radar in front of any other underlying threat actor, escalating those threat factors exponentially - even into the realm of an Advanced Persistent Threat.

Competitors

Motivation Monetary | **Skill** Various | **Likelihood** Moderate | **Impact** Extreme

Competitors have a high motive toward both attack and exploitation scenarios, though the latter is much more common. They often don't have much skill on their own and are more likely to seek out Hackers for Hire to get the job done. They are even more likely to seek out published or for-purchase data provided by other threat actors. Once successful, Competitors can deal immense damage in many different hidden ways.

Activists

Motivation Political | **Skill** Various | **Likelihood** Low | **Impact** Varies

Activists are politically motivated, often due to principled opposition to some aspect or use of the system or its stakeholders. Any reason why an idea, app, system, or the data residing on it might be subject to social or political controversy is cause to take the aspects of an activist threat seriously.

Terrorist Groups

Motivation Political | **Skill** Various | **Likelihood** Low | **Impact** Varies

Similar to Activists, political motivations drive Terrorist Groups operating in the realm of cyber attacks, though their end goal differs. Where espionage or activist actors often seek to expose information, destruction of systems and infrastructure dominates the tactical agenda of Terrorist Groups, along with damage to the reputation of their targets.

Nation States

Motivation National | **Skill** Very High | **Likelihood** Moderate | **Impact** Extreme

We already live in a world where every developed country sends people to college with the career ambition of hacking the military, infrastructure, and industrial complex of other countries. By their very nature, startups represent a target demographic for the intelligence services and military of foreign nations engaging in exploitation and attack strategies of computer-based espionage and cyber warfare. What might initially seem like a generic job costing or decision support tool could quickly become vital to national security if used on critical projects, a fact that is not lost on the highly talented and well-funded teams working on behalf of an adversarial nation. They have no qualms about getting an early foot in the door at the inception of any startup in order to capture emerging technologies.

Insiders

Motivation Personal | **Skill** Various | **Likelihood** Moderate | **Impact** Extreme

Since the threat spectrum is structured mostly according to capability, Insider threats not only have a place on this list, but also one of extreme impact severity due to the access and institutional knowledge Insiders possess. Also, Insiders don't need to be adversarial or laden with malicious intent to be a threat. By virtue of being human, Insiders can make physical, social, or technical mistakes that can lower the defenses or increase the attack surface of a system or organization dramatically. This is why security awareness training and other efforts to strengthen the 'human firewall' is just as important as background checks and employee monitoring.

SOLUTION: A Holistic Approach

Threats can be varied, hidden and elusive. There is very little a startup can do to eliminate or even identify most actors in their threat landscape. This makes prevention a vital component of the overall security strategy. The mantra of defensive security is that it must be built in to the system from the beginning and not bolt on as an afterthought. This holistic approach is the impetus for the Secure Web Application Development Lifecycle:

Secure Web Application Development Lifecycle

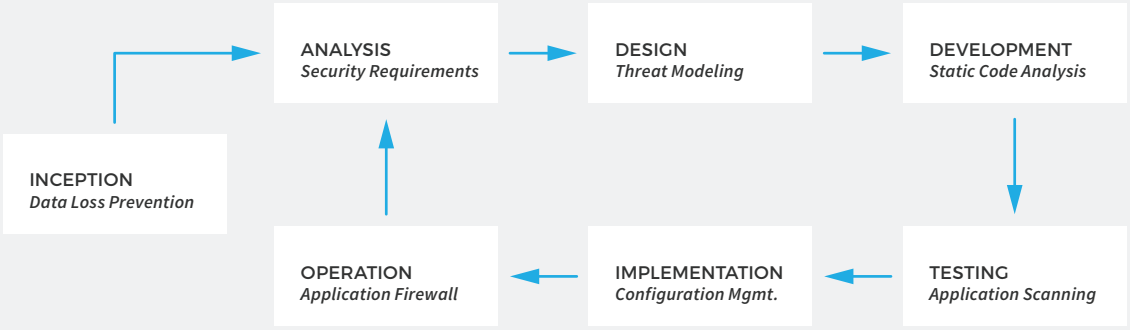

Figure 2: Cyclical model of the Secure Web Application Development Lifecycle

Inception – Data Loss Prevention

Startups should never overlook the security needs of their project, especially the initial OpSec (operations security) required at the very beginning. Startups must remember that unencrypted plain SMTP email is akin to communicating via postcards, and that data scraping by both untargeted and targeted threats can put sensitive details and strategies out in public or in the hands of competitors.

Team services like Basecamp, SharePoint, and Atlassian offer easily established spaces for keeping teams organized yet still provide controls and protections that can be centrally managed. More complex and costly Data Loss Prevention tools are often the last consideration as a confidentiality tool for startups, but should actually be used very early on as part of a strategy for inception management and confidentiality.

Analysis – Security Requirements Traceability

This is key to integrating compliance and other security goals into the system holistically. Developers rely on requirements for everything from job costing to test case development. By integrating security requirements alongside functional system requirements, the project can easily keep tabs on the holistic incorporation of security controls and quickly discern where and when anything goes off track.

Design - Application Threat Modeling

Application Threat Modeling is essential to understanding and properly prioritizing specific attack vectors and defensive measures unique to the application. If ignored during the design phase, such efforts are often very difficult to catch up on. The helpful Open Web Application Security Project (OWASP) recommends a three step process for threat modeling to “decompose the application, determine and rank threats, then determine countermeasures and mitigations”.

Threat categorizations like STRIDE (Spoofing, Tampering, Repudiation, Information disclosure, Denial of service, Elevation of privilege), threat risk ranking models like Microsoft’s DREAD (Damage, Reproducibility, Exploitability, Affected users, Discoverability) and risk models like OWASP’s own Risk Rating Methodology (RRM) go a long way toward both assisting and standardizing the application threat modeling and risk management practices.

Development – Static Code Analysis

The development phase is where most vulnerabilities are unwittingly created, so there is no better place to weed them out early in the development process. Static Code Analysis tools scan source code to discern security or compliance weaknesses and provide guidance on remediation of any findings. They can be used anywhere from aggregate unit testing on a per-task basis to scans of larger batches of code before pressing the build button. The ideal scenario involves leveraging both approaches, and also planning for remediation efforts in the project schedule, with awareness that any change or addition of new code carries the potential for new security-related bugs.

Testing – Web Application Security Scanning

Web Application Security Scanning should be employed to test the security capabilities of the app while functional QA testing is also taking place. These tools operate over HTTP and can rapidly spider through an application, finding thousands of attack vectors related to input validation, session management, exception handling, platform configuration and more. Each is then tested systematically with report output describing findings and recommendations along with traceability to security compliance controls.

Popular and effective scanners exist in both the open source and commercial software realms. It helps to use the same tools that your final compliance auditing team will employ to avoid overlooking a finding.

Implementation – Configuration Management

The key to a secure implementation is solid Configuration Management and Change Control practices. Without keeping track of the system and its changes, too much can easily go wrong in the realms of confidentiality, integrity, availability and vulnerability. Startups can begin on firm footing with a quality Configuration Management Plan and can ensure it continues with effective Change Control reviews and procedures. This is one area where vital operational and security drivers converge.

Operation – Web Application Firewall

Security tools that rely on heuristic behavior-based threat detection are essential as attackers have become adept at evading the more traditional pattern-based technologies. A web application firewall (WAF) is designed specifically to address many of the attacks and vulnerabilities that administrators and web developers simply cannot shake off or remediate fast enough.

A WAF that is behavior-based by design is a powerful protection mechanism that can withstand efforts to bypass more traditional signature-based web application firewalls. WAFs also provide sizeable risk reductions in security and compliance assessments by serving as a reliable mitigation to underlying weaknesses in the system that may take time to fully remediate.

CONCLUSION: A New Beginning

By their very nature, startups building web applications have a unique opportunity to stay ahead of the security curve by understanding and evaluating threats through the lens of risk assessment, designing the application for higher threat resistance through defense in depth, and holistically integrating robust security controls and policies from the point of inception. Security awareness and training to strengthen the 'human firewall' is also a crucial component. The current and shifting sands of the threat landscape make these practices vital to the success of any project.

ADDITIONAL RESOURCES

REFERENCES

1. BugTraq (http://seclists.org/bugtraq)
The premier general security mailing list and part of the epicenter of the information security community. Vulnerabilities are announced and discussed here in an orderly fashion via manually moderated/approved messages.

2. Full Disclosure (http://seclists.org/fulldisclosure)
A public, vendor-neutral forum for detailed discussion of vulnerabilities and exploitation techniques, as well as tools, papers, news, and events of interest to the community. The relaxed atmosphere of this quirky list provides some comic relief and certain industry gossip. More importantly, fresh vulnerabilities sometimes hit this list many hours or days before they pass through the Bugtraq moderation queue.

3. Metasploit (https://www.metasploit.com)
As the world's most used penetration testing software, Metasploit helps analysts verify vulnerabilities and manage security assessments. Like most security tools, it can be used to attack systems as well, both legitimate testing and for unauthorized use.

4. Sutton's Law (https://en.wikipedia.org/wiki/Willie_Sutton#Sutton.27s_law)
When asked by a reporter why he robbed banks, Irish-American outlaw Willie Sutton was said to have casually replied: "Because that's where the money is."

RESOURCES

- Open Web Application Security Project (OWASP)
  https://www.owasp.org
- US Computer Emergency Response Team (US-CERT)
  https://www.us-cert.gov
- Federal Risk and Authorization Management Program (FedRAMP)
  https://www.fedramp.gov
- NIST Computer Security Resource Center (CSRC)
  http://csrc.nist.gov
- NIST Cybersecurity Framework (CSF)
  https://www.nist.gov/cyberframework
- National Initiative for Cyber Education (NICE)
  http://csrc.nist.gov/nice/resources.html