How Application Security Fits Into the SECURITY ECOSYSTEM

VERACODE

WHAT'S INSIDE

INTRODUCTION

The sophisticated technology used to power your business also opens your company to the outside world, making it vulnerable to cyberattackers and breaches. As a result, organizations like yours have employed a complex system of security tools and services that combine to create an ecosystem-like environment. And like a natural ecosystem, the security ecosystem must be in balance with how you do your business to properly reduce the risk introduced by new technologies. Understanding the complete security ecosystem and how to balance its many components is a critical part of keeping your confidential data secure.

MORE TECH, MORE RISK

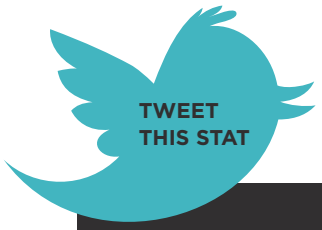
Your business runs on technology — all businesses do, and have for some time. Why? Because technology like email, file shares, websites, voice over IP, centralized datacenters and even Internet access makes employees more productive, customers happier, marketing reach further and businesses more successful. With these and other technologies, businesses are able to move faster than ever before. But as technology proliferated, so did the risks that this technology could be used against the company.

Cyberattackers are using weaknesses in your technological infrastructure to breach your organization and steal company and customer data. This has been true for as long as there have been computers in the office.

But, this does not mean companies haven't fought back. As each new technology was introduced, and cyberattackers found ways to infiltrate the technology, security professionals have found ways to protect their companies. The ping-pong effect of companies introducing new technologies, cyberattackers finding ways to breach them, companies implementing security tools and services to protect their infrastructure, and then cyberattackers finding even newer methods for infiltration continues to this day. It is a never-ending battle, out of which grows a complex ecosystem of security technologies. These interdependent systems all protect and secure different aspects of your organization's technology in order to reduce your company's risk of being breached. As the technology expands, with new "species" being introduced, so does the security ecosystem.

DID YOU KNOW?

There have been 595 new reported web application vulnerabilities in 2015, according to **Risk Based Security's VulnDB,** of which 291 were high severity by their CVSSv2 score, 198 had no known solution and 18 didn't even have a vendor response.



"There have been 595 reported new web application vulnerabilities in 2015."

ACCORDING TO RISK BASED SECURITY'S VULNDB

KEY TAKE-AWAYS

- **Cyberattackers are using weaknesses in your technological infrastructure to breach your organization and steal company and customer data.**
- **The ping-pong effect of new protection methods and escalating attack methods continues today.**
- **It is a never-ending battle, out of which grows a complex ecosystem of security technologies.**

WHAT DOES THE SECURITY ECOSYSTEM LOOK LIKE?

The **Open Systems Interconnection model (OSI model)** is a conceptual model that characterizes and standardizes the communication functions of a telecommunication or computing system without regard to their underlying internal structure and technology. Its goal is the interoperability of diverse communication systems with standard protocols. The model partitions a communication system into abstraction layers. (The original version of the model defined seven layers.)

The security ecosystem exists to protect the creation and delivery of business goods and services. As such, its role is extremely broad — from physically locking doors to data execution prevention on the CPU. This is known as door-to-core protection.

The security ecosystem can be categorized into eight layers based on the Open Systems Interconnection (OSI) model, a conceptual model of the structure, technology and interactions of systems. In security, we know that it is during the interpretation of interactions when mistakes are often made.

These layers are, starting from the top layer:

8. HUMAN

Here we have users such as employees, clients and vendors. Direct access to systems isn't necessary to attack; sometimes trust is abused with attacks like phishing emails to trick users into sharing usernames and passwords, and the access is indirect.

7. APPLICATION

This layer includes the design, development, upgrade and maintenance of an application. Attacks at this layer are against the application itself or at the client side of the remote users, generally through a web browser.

6. PRESENTATION

This layer is a translation layer between networking and the application. Here you find interpretations of interactions such as encoding, compression and encryption that are most often abused to glean information for further attacks.

5. SESSION

At this layer, the connection and transmission of data takes place. This is the area where attacks occurring against authenticated access is a major problem. At this level, you find denial-of-service attacks against services, hijacking legitimate access logins and the use of spoofing, which is connections from fake addresses to distract or reveal network information.

Each of these security layers acts in balance to protect the entire ecosystem or environment. If you remove one piece or restrict resources, or if a piece fails, the entire ecosystem can become unstable or insecure.

4. TRANSPORT

This part of the stack ensures reliable transmission of data between computers. The attacks against this layer include denial-of-service and various man-in-the-middle attacks to read, change, redirect or corrupt data.

3. NETWORK

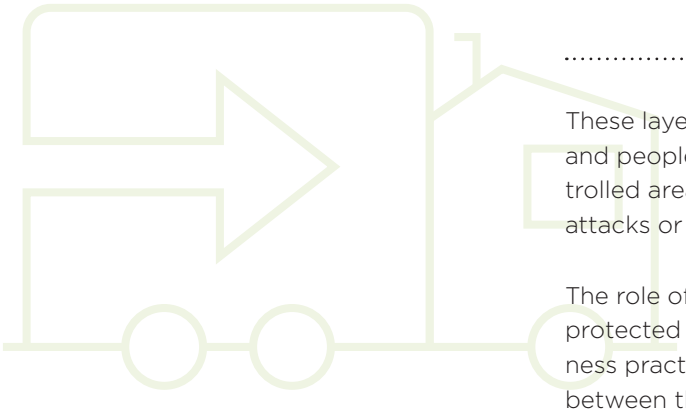
This is the packet layer where network addressing, routing and other traffic control takes place. Attacks at this level include protocol flooding like using ICMP messages to overload a target and sniffing traffic to capture and read contents such as logins and passwords.

2. DATA LINK

At this layer, the data is just one level above the bare metal and silicon of the hardware. This layer moves the data from software to hardware. Threats at this level are packet flooding and poisoning attacks against hardware, such as network switches to gain access to traffic on other networks.

1. PHYSICAL

This is the lowest layer where the hardware shares the same physical, real-world space as the user. Therefore, attacks at this layer are also physical and include destruction, obstruction, manipulation of trusted or intended use and malfunction.



These layers are a good representation of how systems, software, networks and people all interact and contribute to the attack surface — the uncontrolled areas where attacks can occur. Each layer is subject to direct access attacks or indirect attacks through abuse of trust.

The role of a security ecosystem is to ensure that all of the layers are protected and that the attack surface is minimized without blocking business practices. That requires a good understanding of the cohesiveness between the levels, the resources needed and the balance required to maintain security, just like the elements of any ecosystem.

KEY TAKE-AWAYS

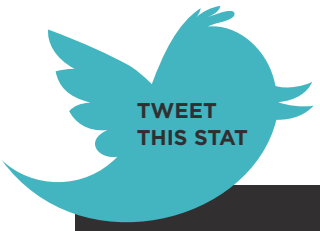
- **The security ecosystem exists to protect the creation and delivery of business goods and services.**
- **The security ecosystem can be categorized into eight layers based on the Open Systems Interconnection (OSI) model.**
- **Each of these security layers acts in balance to protect the entire ecosystem or environment.**
- **If you remove one piece or restrict resources, or if a piece fails, the entire ecosystem can become unstable or insecure.**

HOW APPLICATION SECURITY FITS INTO THE ECOSYSTEM

Applications, the latest invasive species

The steady growth of technology as a business driver has ushered in a new era for companies of all sizes. Today, regardless of what your company's core business may be (manufacturing, financial services, banking, healthcare), your organization is a software company. In the past, companies purchased hardware and technology to run the business more efficiently. Today, the application revolution that is currently sweeping the world means that companies of all sizes are relying more heavily on the applications they build, buy and download.

Even companies like GE, which are traditionally seen as manufacturers, are producing more software than ever before. As this "species" of technology invades and integrates to become part of every company's technology environment, the security ecosystem must adapt to include the application security solutions that will help reduce risk and keep the ecosystem in balance.



"Web and mobile applications account for more than a third of data breaches."

ACCORDING TO VERIZON'S DATA BREACH INVESTIGATIONS REPORT

Applications introduce risk into the ecosystem

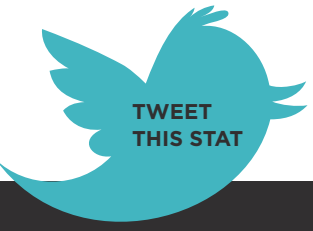
If applications are the new species in the business environment, they are also the area that has the potential for throwing the system out of balance, introducing risk. The newness and very nature of how Internet-enabled applications work — making it possible for your company to interact effectively and efficiently with the outside world — increase the risk of cyberattacks. In fact, web and mobile applications account for more than a third of data breaches (source: 2014 Verizon Data Breach Investigations Report).

"On our current trajectory, GE is on track to be a top 10 software company."

JEFF IMMELT, GE CEO

Prevalence of applications means security ecosystems are struggling

Applications are running your business, but without careful planning, they could be ruining your business. The balance in the security ecosystem needs to shift to accommodate this new reality of applications. Many organizations wrongly assume that their other security measures, such as network security, Web Application Firewalls (WAFs) or data leakage prevention tools, protect them from cyberattackers. Recent high-profile breaches show this assumption to be false.



"Without specific application defenses in place, an organization would only stop 18 percent to 43 percent of the last 24 months of exploits."

ACCORDING TO PICUS SECURITY

According to research by Picus Security, which tests live exploits against various infrastructure protection devices for security effectiveness, without specific application defenses in place, an organization would only stop 18 percent to 43 percent of the last 24 months of exploits. However, with the inclusion of application defenses, this success rate can rise to 72 percent to 96 percent.

According to Akamai's "State of Internet Security" report, "application-layer attacks are growing much more rapidly than infrastructure attacks." And with companies in all industries relying more and more on applications as a source of innovation and business efficiencies, the number of attacks against the application layer will only continue to grow.

In 2014 alone, there were eight major breaches through the application layer, resulting in more than 450 million personal or financial records stolen.

KEY TAKE-AWAYS

- **Regardless of what your company's core business may be, your organization is a software company.**
- **Web and mobile applications account for more than a third of data breaches (source: 2014 Verizon Data Breach Investigations Report).**
- **According to Picus Security, without specific application defenses in place, an organization would only stop 18% – 43% of the last 24 months of exploits.**
- **In 2014 alone, there were eight major breaches through the application layer, resulting in more than 450 million personal or financial records stolen.**

"Companies can put all of the other cybersecurity controls in place, but if there are application weaknesses, hackers have the will and time to find and exploit them. The issue simply cannot be neglected anymore."

CHRIS WYSOPAL, VERACODE CISO AND CO-FOUNDER

THE SECURITY ECOSYSTEM IS FRAGILE

A security ecosystem is fragile by default. Like all ecosystems, it depends on a delicate balance of controls, interactions and vulnerabilities. According to the Open Source Security Testing Methodology Manual (OSSTMM), interactions require controls to minimize the attack surface; however, more controls can also lead to more interactions, which means a greater attack surface. This is known as the Attack Surface Paradox.

Therefore, adding application security into an established security ecosystem requires maintaining that balance between controls and attack surface. When done correctly, application security will not only create balance, but will actually help other forms of security thrive.

If you give one security layer more weight or priority over other layers, this causes an imbalance in the ecosystem. Typically, the reason for giving one system priority over others is that the assets it touches bring in revenue or have more visibility, which makes the system seem more important than it may actually be. However, attacks to systems can come through all levels, which is why giving priority to some leaves attackable gaps in others, allowing access into your network. Additionally, by giving one area higher priority, you end up making it more difficult to justify investing in the other security layers.

The main goal of introducing application security is to protect the business. Since applications tend to tie together multiple systems across the network and across many types of users, you need to give equal attention to application security. This is because application security is controlling the design, development, upgrade and maintenance of an application.

Therefore, by default, application security actually impacts every layer of the security ecosystem. As a result, it ends up becoming an equalizer of the security ecosystem rather than a disruptor.

Adding application security to the ecosystem

The introduction of application security shifts the focus from vulnerability management to proactively reducing the incidents of vulnerabilities in applications. While both are important, applications often face attacks that have no patch. This leads to the need to proactively design the architecture to limit types of interactions and to focus on prevention by improving security at the development phase. This includes virtualization, reverse proxies, bastion hosts, SSL termination end points and robust test environments.

KEY TAKE-AWAYS

- **Adding application security into an established security ecosystem requires maintaining that balance between controls and attack surface.**
- **Application security actually impacts every layer of the security ecosystem. As a result, it ends up becoming an equalizer of the security ecosystem rather than a disruptor.**
- **The introduction of application security shifts the focus from vulnerability management to proactively reducing the incidents of vulnerabilities in applications.**

CONCLUSION

Like any ecosystem, the security ecosystem exists in a delicate balance. When a major shift is introduced, like the explosion of applications and their interactions with the outside world, it becomes necessary for security professionals to assess how they can rebalance the ecosystem so there is harmony, also known as reduced risk.

Security professionals act as "environmentalists" to the security ecosystem, carefully balancing the security solutions they need with the business operations to reduce the cyber-risks their companies face. Security needs to be balanced between controls and operations because every interaction matters. Applications bring many more and new types of interactions on all layers. Introducing the methods of application security addresses these interactions and benefits the entire security ecosystem.

And like an environmentalist studying a complex ecosystem, it requires specific knowledge, expertise, tools and dedicated effort to find that perfect balance.

VERACODE

The Most Powerful Application Security Platform on the Planet

Veracode's cloud-based service and systematic approach deliver a simpler and more scalable solution for reducing global application-layer risk across web, mobile and third-party applications. Recognized as a Gartner Magic Quadrant Leader since 2010, Veracode secures hundreds of the world's largest global enterprises, including 3 of the top 4 banks in the Fortune 100 and 20+ of Forbes' 100 Most Valuable Brands.

LEARN MORE AT WWW.VERACODE.COM, ON THE VERACODE BLOG, AND ON TWITTER.