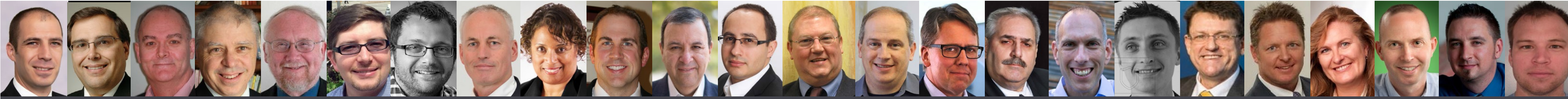

Mighty Guides

Securing Your Network and Application Infrastructure

Part 4: Protecting Against APTs and Application-based Attacks

2 Experts Share Their Secrets

SPONSORED BY:

FORTINET

FOREWORD

Network security challenges are evolving faster than ever as a result of new technologies and application complexity. In addition, many old issues continue to plague organizations, from simple password security to keeping software up-to-date.

This collection of 24 essays covers a broad array of topics grouped into five major areas, ranging from the necessity of planning your network security up front to the new challenges that social engineering and other advanced, persistent threats bring. A major theme throughout many of them is the loss of the perimeter and the effectiveness of traditional defenses. Bring Your Own Device (BYOD) and cloud-based services open many holes in an organization's network that require a rethinking of security to protect the data, not just the methods of access.

Fortinet's Cyber Security platform can address most of the problems outlined in the essays in this e-book. Our ASIC-powered FortiGate firewalls deliver the industry's fastest Next Generation Firewall (NGFW) performance and are the foundation of an end-to-end security solution that spans your users, network, data centers, and the cloud. For the problems we can't solve directly, we offer tools such as enforcing business policies on password changes and vulnerability scanners for your applications to help you catch weaknesses.

We hope you find these essays as interesting and thought provoking as we do and that they can help you improve your network and application security defenses.

INTRODUCTION

For all the attention data security has received in recent years and all the technical advances in risk detection now available to protect network infrastructures, you might imagine that data are safer than ever before. Unfortunately, the number of recent, frighteningly large data breaches contradicts that notion. In the past 18 months alone, we have seen breaches at Adobe, eBay, JPMorgan Chase, Target, Home Depot, Community Health Services, and the US Government that together compromised more than 500 million records. Will the world ever be a safe place for the data so vital to businesses and individuals?

With the generous support of Fortinet, we have created this e-book to help you better understand the security challenges that business—and midsized businesses in particular—face today. This e-book is a compilation of responses to the following question:

What are the greatest challenges you face in securing your network and application infrastructure?

A range of industry analysts, consultants, and hands-on security experts provided responses to this question. They offered fascinating insights into the security challenges we face today—security issues made even more challenging because of the changing character of infrastructure and its loss of network perimeter, rapidly evolving application environment, lack of security awareness among users, and the increasing complexity of security solutions. Attacks and data theft have also become a big business underwritten by sophisticated, well-funded entities.

Security and vigilance are a never-ending battle, but I trust you will find the many perspectives provided by those who are on the front lines useful as you work to secure your own business infrastructures.

All the best,
David Rogelberg
Publisher

Mighty Guides

Mighty Guides make you stronger.

These authoritative and diverse guides provide a full view of a topic. They help you explore, compare, and contrast a variety of viewpoints so that you can determine what will work best for you. Reading a Mighty Guide is kind of like having your own team of experts. Each heartfelt and sincere piece of advice in this guide sits right next to the contributor's name, biography, and links so that you can learn more about their work. This background information gives you the proper context for each expert's independent perspective.

Credible advice from top experts helps you make strong decisions. Strong decisions make you mighty.

© 2015 Mighty Guides, Inc. I 62 Nassau Drive I Great Neck, NY 11021 I 516-360-2622 I www.mightyguides.com

Protecting Against APTs and Application-based Attacks

In cybersecurity, there's A LOT OF HYPE...

...and then there are facts.

Flashy marketing has a way of clouding the truth: slow is broken. You don't have to choose between having a strong security posture and having optimal network performance to power your business.

You can have both—but only from us.

97.3% effective breach detection

5X NGFW performance

#1 unit share worldwide in network security

Over 200 zero-day attacks discovered

Get a Cyber Threat Assessment today and get the facts about your security posture.
www.fortinet.com/ctap

FORTINET®

Security Without Compromise

APPLICATIONS REPRESENT TODAY'S GREATEST SECURITY RISKS

MIKHAEL FELKER

Director of Information Security,
VC backed eCommerce

Mikhael Felker is the director of information security at a growing venture in Santa Monica, California. His professional experience is a confluence of information security, privacy, teaching, technical journalism, and nonprofit leadership in such industries as defense, health care, nonprofit/education, and technology. Mikhael received his M.S. degree in information security policy and management from Carnegie Mellon University and B.S. degree in computer science from UCLA.

Twitter | Blog

Securing Your Network and Application Infrastructure

24 Experts Share Their Secrets

FORTINET

Download the full eBook:

Securing Your Network and Application Infrastructure

In a modern network and application infrastructure, the application has become the greatest point of risk for several reasons. One is that there is a proliferation of apps, made possible because apps are easier to build than ever. The number of apps appearing in a typical business environment is increasing, and these apps are evolving rapidly. Unfortunately, the resources available to address any security issues these apps may create is comparatively fixed. Several business dynamics aggravate the problem of application security.

There was a time when the infrastructure was on premises and development cycles were not as fast as they are today. In such an environment, securing the infrastructure was easier. Now, with complex hybrid environments and demand for rapid app development cycles, it is much more challenging to build secure apps in the time in which they are needed. Each business unit might have its own environment and work with its own vendors, and these environments are constantly changing. IT staff create and tear down virtual private networks.

> *"Fixing known flaws . . . comes down to prioritizing development efforts for revenue-generating app features over maintenance."*

KEY LESSONS

1 THE NUMBER OF APPS APPEARING IN A TYPICAL BUSINESS ENVIRONMENT IS INCREASING, WHILE THE RESOURCES AVAILABLE TO ADDRESS SECURITY ISSUES THOSE APPS MAY CREATE IS COMPARATIVELY FIXED.

2 EVEN IF YOU CAN NARROW A LIST OF KNOWN FLAWS TO THE HIGHEST-RISK ITEM, YOU STILL MUST PRIORITIZE THAT FIX AGAINST THE REVENUE POTENTIAL OF BUILDING NEW FEATURES.

APPLICATIONS REPRESENT TODAY'S GREATEST SECURITY RISKS

With a real-time picture of the environment, organizations can focus on the highest security priorities, but gaining that total view of the environment is difficult. Products are available that help aggregate a view of the business environment. Analytics and visualization tools can give IT staff a snapshot of the environment, which they can then use to prioritize security efforts.

Even with snapshots of a complex, ever-changing environment, though, other challenges to building secure apps exist related to prioritizing development efforts and the allocation of development resources. Regarding prioritization, let's assume that the IT organization knows every vulnerability in an app and fully understands the business use cases subject to abuse. The IT organization must prioritize fixing those flaws over building new functions, so it comes down to prioritizing development efforts for revenue-generating app features over maintenance. Even if IT can narrow a list of known flaws to one high-risk item to fix, they must still prioritize making that fix against the revenue potential of building new features.

Compounding the prioritization problem is resource allocation. When looking at overall app security, the organization must look at the broad spectrum of app services, mobile apps, and application programming interfaces. It must also consider the app environment—on premises, Platform as a Service, or Infrastructure as a Service. There is such pressure to build and launch apps quickly that organizations often lack the resources to test the app in all the environments in which staff may use it.

This combination of a growing number of apps, allocating resources to build and test for increasingly complex hybrid environments, and prioritizing security fixes against developing new revenue-generating features is a recipe that makes apps perhaps the greatest security risk businesses face today. With this security challenge in mind, it is more important than ever to involve information security professionals at the earliest stages of business projects, including security and compliance requirements, and to minimize risk and project rework. It is also important to leverage existing standards, frameworks, and methodologies such as the National Institute of Standards and Technology and the International Organization for Standardization to ensure that projects have a security baseline.

> “*It is more important than ever to involve information security professionals at the earliest stages of business projects.*”

DELAYED THREAT DETECTION AND SLOW RESPONSE POSE THE GREATEST THREATS

ERLEND OFTEDAL

Senior Security Consultant,
F-Secure

Erlend Oftedal has worked as a software developer and security tester for more than 10 years. He has spoken at several security and developer conferences and also develops open source security tools. Erlend is the head of the Norwegian OWASP chapter.

Twitter | Blog

Securing Your Network and Application Infrastructure
24 Experts Share Their Secrets
FORTINET

Download the full eBook:
Securing Your Network and Application Infrastructure

KEY LESSONS

1 AS LONG AS VULNERABLE LEGACY APPLICATIONS EXIST, DEVELOPERS MAKE MISTAKES, AND USERS DO THINGS THEY SHOULDN'T, ATTACKERS WILL GET INTO THE SYSTEM.

2 NEW TOOLS ENABLE DEVELOPERS TO BUILD ACTIVE SECURITY MONITORING INTO THE APPLICATIONS THEMSELVES.

It is important to recognize that no matter how many protections we build into our infrastructure, we will always have vulnerable systems. The real security threat comes from not detecting attacks soon enough and not responding to them quickly enough. Many of the highest-profile security breaches in recent years went on for many months before they were detected.

So, what contributes to insecure networks and infrastructure? A big factor is the growing complexity of networks and software environments. Businesses often have a variety of systems they have acquired over the years, including applications built on old frameworks and libraries that no one in the company knows anything about any more. Sometimes, the original manufacturer of an application is no longer in business, and the company would rather develop new code than fix old vulnerabilities.

Software itself is becoming more complex and more dependent on third-party code. Ten years ago, according to studies, 80 percent of code in a new application was custom built and 20 percent came from libraries.

> *“No matter how many protections we build into our infrastructure, we will always have vulnerable systems.”*

DELAYED THREAT DETECTION AND SLOW RESPONSE POSE THE GREATEST THREATS

Today, 20 percent of new applications are made with custom code, and 80 percent of the code comes from libraries. Application development has changed to include more security testing during the development process, with tools that detect vulnerable library code and security routines built in at the unit testing stage. Still, developers make mistakes. Users make mistakes, too.

As long as vulnerable legacy applications exist, developers make mistakes, and users do things they shouldn't, attackers will get into the system. The best protection against these threats is early detection and rapid response. Companies rely on solutions such as next-generation firewalls and honeypots to protect against known threats and look for suspicious activity that may indicate a previously unknown threat. A new approach to software development that may be even more effective for some kinds of applications involves new tools that enable developers to build active security monitoring and sensors into the applications themselves. If the application detects any violation of its known operational behavior, it can send alerts, block an activity, or stop the application altogether. Every application would be built with security checks specifically designed to protect that application against illegal behaviors. The advantage over generic security solutions is that generic solutions never know exactly how an authorized application is supposed to behave.

As our lives become more dependent on software at work, in our homes, and even in our cars, it is essential that we have visibility that allows rapid detection, quick response to contain attacks of all kinds and fast deployment of mitigations when vulnerabilities are uncovered.

> “*The best protection against these threats is early detection and rapid response.*”