THE REAL ROOT CAUSES OF BREACHES

Security and IT Pros at Odds Over AppSec

PREVOTY

EXECUTIVE SUMMARY

Breaches still happen, even with today's intense focus on security. According to Verizon's 2016 Data Breach Investigation Report[1], there is actually a rise in Web application attacks, with over 40 percent of breaches coming through Web applications. In an ideal world, applications would always be coded securely, pass all vulnerability scans and penetration tests and never encounter zero-day attacks. But this is not the reality. Why are breaches on the rise? Why are applications insecure? We sought to determine what is really going on through a survey of over 1,000 IT and security professionals and created this report to share our findings.

Security and IT professionals are at odds in three major areas:

01

IMMEDIACY OF UPDATES

Half of IT professionals update applications once a month whereas half of security professionals feel they need to update applications at least once per day, if not multiple times a day.

02

UPDATING SECURITY SOLUTIONS TAKES A TOLL ON TIME

Both IT and security professionals spend significant amounts of time tuning existing application security solutions, in fact, that's where security professionals spend over 80 percent of their time, and IT professionals almost 40 percent of their time, leaving both groups with little time for other duties.

03

VULNERABILITY BACKLOGS - MASSIVE OR NON-EXISTENT?

Nearly all (93 percent) of security professionals report having up to 5,000 vulnerabilities in their backlogs, and 44 percent of IT professionals report that they have NO vulnerability backlogs.

The objective of our research was to understand what is happening on the front-lines of security, the day to day life of those in the trenches. We found a huge gap between IT and security professionals, and the perpetuation of never-ending security issues, such as breaches and attacks. The research begs the question, how can we close the gap? Is this the real root cause of security breaches? What room is there for innovation? We hope you will find the report informative and insightful as we did. Tweet us your feedback @Prevoty.

Best regards,

Arpit Joshipura
VP Product and Strategy, Prevoty

OVERVIEW

One of the greatest issues for businesses is security. Protecting data and applications has always been a struggle. The issue is not **IF** a breach will happen, but **WHEN.**

New and developing technologies are being developed to remediate the challenge. But are new technologies enough to combat the never-ending headache that is security? Are the efforts of IT and security professionals making applications any safer?

Prevoty surveyed over 1,000 IT and security professionals to learn how those in the trenches are approaching application security on a daily basis, as well as the nature of their struggles and what they would change about the process.

Findings revealed that security professionals are putting in tremendous effort to protect their applications, but it is not enough. Additionally, IT professionals are not spending nearly the same amount of time, or exerting the same amount of effort, that security professionals are devoting to the issue of security. What impact does this disparity have on security? Could it be that the divisive disconnected way we approach security might be leaving the door open for breaches?

SECTION ONE

The Divide Between IT Professionals and Security Professionals

We know that those who work in IT span from general IT professionals, to security, to application developers and beyond. This research reveals that when it comes to perception and implementation of security, there is a wide divide between general IT professionals and specialized security professionals.

THE DEEP DIVE

VISIBILITY INTO VULNERABILITIES

IT PROFESSIONALS	SECURITY PROFESSIONALS
39 PERCENT don't feel their organizations have visibility into what vulnerabilities are being exploited in their applications	**92 PERCENT** feel they have visibility into the vulnerabilities, but it takes time to discover them

FREQUENCY OF APPLICATION UPDATES

IT PROFESSIONALS	SECURITY PROFESSIONALS
50 PERCENT update applications once every **ONE TO SIX MONTHS**	**52 PERCENT** update applications at least **ONE OR MORE TIMES PER DAY**

Security professionals know that today's security solutions need constant and never-ending updates and patches to keep the company's data and applications secure, yet half of IT professionals report that they only update applications once every one to six months. Compare that to the practices of security professionals where 52 percent of security professionals update applications at least once a day, if not multiple times a day, and 82 percent of security professionals update applications at least once a week.

ADDRESSING VULNERABILITIES

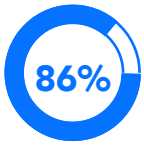
IT PROFESSIONALS	SECURITY PROFESSIONALS
26% Address application vulnerabilities **RARELY**	90% address application vulnerabilities **OFTEN**, to review, prioritize or remediate them

UNDERSTANDING APPLICATION SECURITY

IT PROFESSIONALS

are unsure if a layered security approach is slowing them down

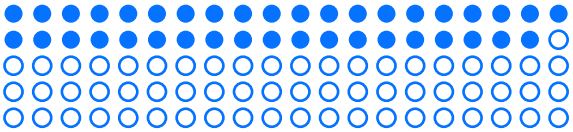
SECURITY PROFESSIONALS



are aware of the effects of a layered security approach

STUCK IN THE DARK AGES

IT PROFESSIONALS



39 PERCENT use next generation firewalls, and **OLD SCHOOL SOLUTIONS**, as their application security solution

SECURITY PROFESSIONALS

Security professionals are investing in newer solutions and methods:

63 PERCENT
use a web application firewall

38 PERCENT
use dynamic application security testing

32 PERCENT
use static application security testing

29 PERCENT
use security incident & event management tools

To address this gap, security professionals believe changes can be made. More than half (55 percent) of security professionals feel that changes could be made to their businesses' approach to application security. Although they feel that the use of application security testing and scanning tools, such as static, dynamic or interactive application security testing (SAST/DAST/IAST) would accelerate or improve their application security, **85 percent reported that their supervisors believe the organization's current security solutions are enough to protect the company's applications and data**. With continued attacks and breaches, how can that be? Is it time for Runtime Application Self-Protection (RASP), where applications will protect themselves?

SECTION TWO

In a Time Crunch, Security Takes a Back Seat

THE TWO WORST CULPRITS - SUPPORTING AND TUNING LEGACY APPLICATIONS

Our previous report, *The Impact of Security on Application Development*, revealed that given the destructiveness of a major data breach, it should be a business priority to make sure that all known application vulnerabilities are being remediated prior to release. However, nearly half admitted to releasing applications with vulnerabilities at least 80 percent of the time, because of pressure to release the application quickly. Think about that percentage for a moment. **80 percent of the time, developers release or update a production application that they are fully aware is vulnerable to attack.**

THE CULPRITS

TIME CONTINUES TO BE AN OBSTACLE TO APPLICATION SECURITY

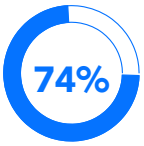
IT PROFESSIONALS

83 PERCENT spend nearly **2.5 DAYS/WEEK** tuning existing application security solutions

SECURITY PROFESSIONALS

97 PERCENT spend up to **4 DAYS/WEEK** tuning existing application security solutions

61 percent of those surveyed described their **BIGGEST CONCERN** with maintaining the security of their application as being **RELATED TO TIME** - either the deployment schedule or time spent supporting legacy applications.



Deployment Schedule

Time Spent Supporting Legacy Applications

CONCERNS WITH MAINTAINING THE SECURITY OF APPLICATIONS

For security professionals, the release of an application does not mean the work is over. In fact, it has really just begun. **58 percent have to update an application at least once a day**. And with limited hours in a day, the backlog of vulnerabilities builds up.

SECTION THREE

The Truth About Vulnerabilities: Massive or Non-Existent?

No matter the amount of time spent maintaining and updating applications, companies still face a backlog of security vulnerabilities that needs to be assessed and addressed. Or do they?

AMOUNT OF VULNERABILITIES BACKLOGGED

UP TO 5,000
Most security professionals

1,000 - 100
Half of IT professionals

NONE
Half of IT professionals

THE CHALLENGE

ADDRESSING SUCH A HIGH NUMBER OF VULNERABILITIES IS VIRTUALLY IMPOSSIBLE

IT PROFESSIONALS

say it takes **TWO DAYS** to fix a newly discovered application vulnerability

SECURITY PROFESSIONALS

say it takes **MORE THAN 24 HOURS** to fix a newly discovered application vulnerability

To put this into perspective, if a company has a backlog of 5,000 vulnerabilities, they will need close to **TWO YEARS** (around 625 days) to address them.

This means that when a security professional recognizes there is a new vulnerability, he or she has two choices: a) prioritize fixing the vulnerability for the next three work days or b) note the vulnerability and plan to address it later, which results in excessive, growing backlogs. It's a never-ending cycle. IT professionals see the situation differently; they don't report huge vulnerability backlogs, but then again, do they have the same visibility as the security professionals? Do they have the same training or knowledge base?

What impact do these challenging perceptions have on a company's security? Clearly, IT professionals are unaware of the depth of difficulties security professionals face on a daily basis. This is underscored by the fact that almost half of IT professionals are unaware that their organization has vulnerability backlogs.

KEY TAKEAWAYS

01 TIME

is a precious resource and the primary pain point when it comes to the maintenance and security of applications; the pressure to release applications quickly (which is causing applications to be released with vulnerabilities), and the time it takes to maintain and tune legacy and existing applications, is far more than IT professionals realize.

02 VULNERABILITY BACKLOGS ARE INEVITABLE

for most security professionals. However, IT professionals are less aware of the backlog and how frequently it needs to be addressed. Could this cause conflict and ultimately lead to the detriment of security? Absolutely.

03 THERE IS A HUGE DIVIDE

between IT professionals and security professionals when it comes to application security and no consensus on best practices.

CONCLUSION

There is no question that security professionals are dedicating a significant amount of time and effort to maintain application security and resolve vulnerabilities, but is it enough? And is the divide between general IT professionals and security professionals too large? Perhaps organizations should foster consensus, awareness, and deeper knowledge about the true need, cost and impact of application security and vulnerability remediations. Having a secure enterprise is more than a perception. Maybe IT professionals, even those not tasked with security, need to up their security game. Because sooner or later, the collective divide between perception and reality needs to shrink dramatically in order to ensure that company data and applications are protected from unwanted attacks or breaches.

ABOUT PREVOTY

Prevoty is dedicated to securing enterprises and the users they serve by monitoring and protecting the applications that are the heart of modern business. By using a LANGSEC-based approach to accurately analyze attacks from inside production applications, Prevoty's products provide real-time application security intelligence and RASP (Runtime Application Self-Protection). These capabilities enable Global 2000 enterprises to dramatically improve remediation of vulnerabilities, enabling security and development teams to work together more effectively, even with agile release cycles.

Prevoty was founded in 2013 and is headquartered in Menlo Park, California. For more information on the company's application security solutions, go to prevoty.com or follow @Prevoty on Twitter.

METHODOLOGY

Prevoty surveyed 1,000 U.S. IT Professionals on their approach to application security. This survey was completed online and responses were random, voluntary and anonymous.

[1]Verizon. (2016). *2016 Data Breach Investigations Report*. Retrieved from: http://vz.to/1NTb7l8

PREVOTY

@prevoty

linkedin.com/company/prevoty