State of the Applications :

Only 11% of Information Security Managers Feel Their Applications are Secure

Table of Contents

1 Introduction

Ofer Maor, Chief Technology Officer, Quotium
Adam Brown, UK Manager, Quotium

Quotium Research team has conducted a study in attempt to better understand the application security market, discovering alarming findings regarding the level of security and frequency of attacks organizations are facing at the application level.

The study was conducted over a period of several months through questionnaires and interviews done with over 500 CISOs, Information Security Directors and Information Security Officers of leading corporates in Europe and in the United States.

As part of the study, participants were asked:

2 "Do applications in your organization have vulnerabilities that hackers could exploit?"

The results were alarming – just over half were positive they are vulnerable and only 11% felt that they were secure. It is important to note that the focus was not whether vulnerabilities exist at all or not, but whether there are ***real, substantial*** vulnerabilities which Hackers may take advantage of.

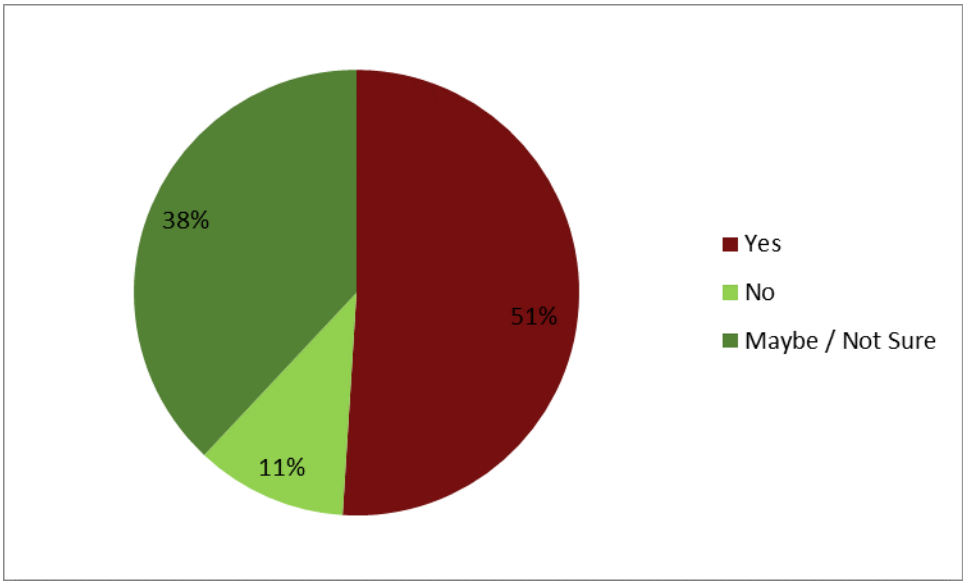

Figure I – "Do applications in your organization have vulnerabilities that hackers could exploit?"

Interestingly enough, when it comes to *other* people's applications, people were a lot more positive of the risk. Over 80% of participants have answered ***Yes*** to the statement *"100% of Off-the-Shelf Applications You Buy Are Vulnerable".*

Another interesting point was the lack of actual knowledge on the state of application security in the organization. A little over third (38%) answered "Maybe" or "Not Sure". This lack of knowledge continued in the following questions, where we tried to learn which applications and being attacks and how frequently. In both cases, almost half of the participants could not provide a well-informed answer.

Nonetheless, taking the answers of participants who were able to provide this information, we have discovered that not only most applications are vulnerable, but that many of them are being targeted on a regular basis.

In the first question, we asked:

3 "What percentage of hacks against your organization are targeted at your applications"?

As already mentioned, almost half (48.6%) answered "Don't Know", yet we were able to learn some interesting figures from the other half. In today's world, where attackers have a wide arsenal of potential attacks against organizations, it was clear to us that applications, while proving as a popular attack vector. Nonetheless, 1 of 5 of pointed out that over ***half*** of all hacks against their organization were targeted at the application level. Approximately 2/3^{rds} pointed out it was over 25%.

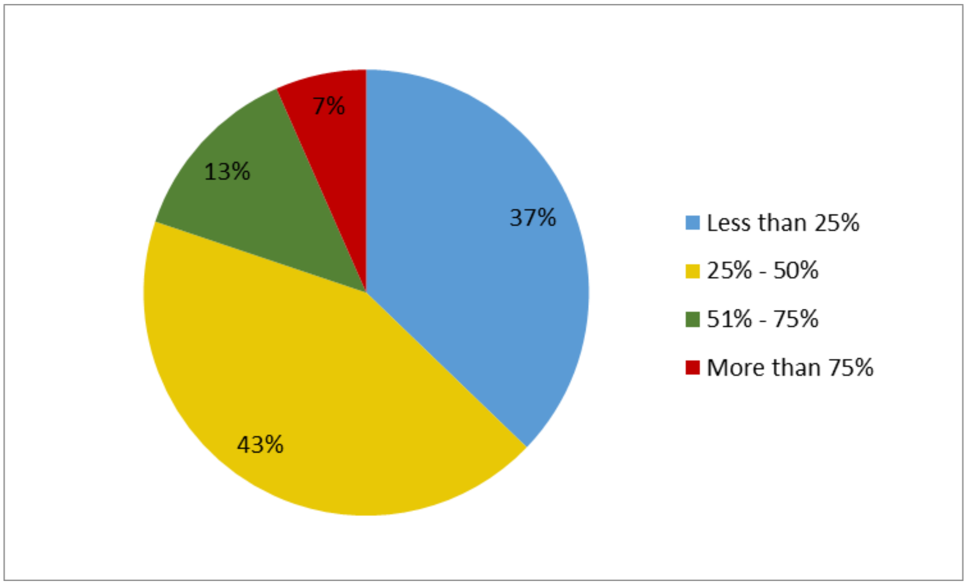

Figure II – "Percentage of hacks against the organization targeted at your applications" (Based on results of 51.4% of participants)

These figures show that applications remain one of the most prominent attack vectors for hackers and cyber attackers.

In the second question, attempting to figure the frequency of attacks, we asked:

4 “How frequently do your applications get targeted?”

Here, again, almost half (45.1%) answered “Not Sure”, indicating again how many organizations have little visibility over the actual attacks taking place against their organizations. Looking at the results of the remaining participants we were able to learn that just over 40% of these organizations get targeted every single day with application attacks. Only 16% feel that they are targeted less than once a year or never.

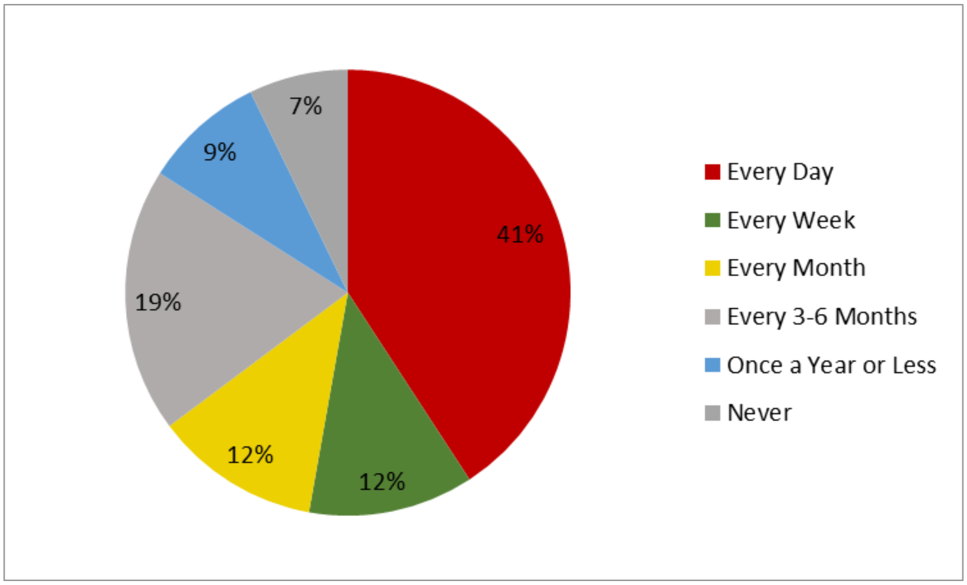

Figure III – “Frequency of Attacks on Applications in Organization”

(Based on results of 54.9% of participants)

While figures in this order of magnitude are not new, they are of some interest when looking at application attacks, where the complexity of attacks often requires more than just automated tools to run, and indicate this is a real threat to organizations.

Further interviews with some of the participants in the study has shown that application vulnerabilities are one of the preferred methods of operations by cyber criminals and attackers, as they are able to target the core business and data of the organization. While we were unable to obtain specific figures, almost all information security managers we have talked with have expressed real concerns in this respect.

5 What are the solutions currently in place to mitigate these security threats?

In the second part of the study, we have attempted to learn what organizations are doing in attempt to mitigate these threats. The results have indicated that only a fraction of organizations (8.63%) do nothing regarding application security (and the majority of these were smaller organizations with less than 1000 employees). As expected, the most common practice used by organizations today is still penetration testing. Almost 2/3rds (66.3%) of organizations are using penetration testing services on a regular basis. Second in line are automated testing tools, mostly application scanners and static code analyzers, used by a little over half (55.7%) of organizations. Web application firewalls are also quite popular, with almost half (47.8%) of organizations using them (although it should be mentioned that for the purpose of this study we have not separated between dedicated WAF solutions and add-on WAF solutions). Following the *Security in Layers* approach, almost half (46.8%) of all participants indicated they are using some combination of the above.

6 Conclusions

One of the most interesting results out study has found is the gap between the effort put into protecting applications and the actual state in which applications are. While almost all organizations invest time, money and energy into protecting applications, using one or more type of service or technology, the majority of applications are still vulnerable and attacked. Most importantly, almost half of the information security managers we have met were unable to provide real insight on the amount of vulnerabilities or attacks done against their applications.

It is clear that application vulnerabilities are still a prominent threat to organizations, and an ever difficult task to deal with. The delicate relationship between the R&D and the security makes application security one of the most difficult tasks at hand for an Information Security Officer. Only by choosing the right practices for protecting applications, organizations can protect themselves against this threat.

7 About Seeker

Seeker is the leader of the new generation of application security testing software. Easily integrating with existing software testing processes, Seeker allows developers to efficiently develop secure applications.

8 About Quotium

Quotium Technologies is a specialist in the development of innovative software solutions to guarantee the security and performance of business critical applications throughout their lifecycle.