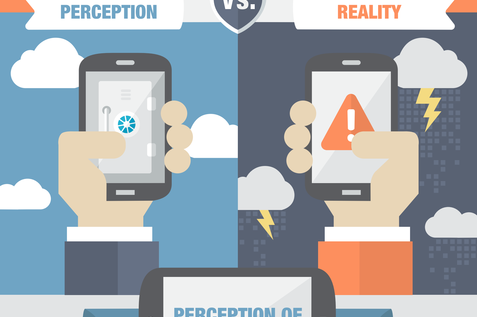
2016

STATE OF APPLICATION SECURITY

ARXAN

PERCEPTION VS. REALITY



PERCEPTION OF SECURITY

1,083 individuals were surveyed in the US, UK, Germany and Japan. 268 were IT executives with security oversight or insight into the mobile health and/or finance apps they produce. 815 were consumers that use mobile health or mobile finance apps.

APPLICATION EXECUTIVES		APPLICATION USERS
87%	I FEEL MY MOBILE APPLICATIONS ARE ADEQUATELY SECURE.	83%
82%	I BELIEVE EVERYTHING IS BEING DONE TO PROTECT MY APPS.	57%
46%	I THINK MY APP WILL LIKELY BE HACKED WITHIN THE NEXT 6 MONTHS.	48%

REALITY OF SECURITY

126 of the most popular mobile health and finance apps from the US, UK, Germany, and Japan were tested for security vulnerabilities using tools from Mi3.[1] Apps approved by regulatory or governing bodies were also included in the security assessment.

90% OF 126 MOBILE APPLICATIONS TESTED WERE VULNERABLE TO AT LEAST 2 OF THE OWASP MOBILE TOP 10 RISKS. [2]

84% OF FDA-APPROVED APPS AND **80%** OF APPS FORMERLY APPROVED BY THE NHS WERE VULNERABLE TO AT LEAST 2 OWASP MOBILE TOP 10 RISKS.

98% OF APPS TESTED LACKED BINARY CODE PROTECTION AND COULD BE REVERSE-ENGINEERED OR MODIFIED.

84% OF APPS TESTED HAD POOR TRANSPORT LAYER PROTECTION AND COULD LEAD TO DATA AND IDENTITY THEFT.

>80% OF APP USERS WOULD CHANGE PROVIDERS IF THEIR APP IS KNOWN TO BE VULNERABLE OR IF A SIMILAR APP WAS MORE SECURE.

50% OF ORGANIZATIONS HAVE ZERO BUDGET ALLOCATED TO PROTECTING MOBILE APPS. [a]

RECOMMENDATIONS

FOR APP EXECUTIVES:

SET YOUR SECURITY BAR ABOVE THE REGULATIONS

Regulatory bodies are lagging cyber criminals. Applications "approved" by trusted sources such as governing bodies like the FDA or the NHS are just as vulnerable as other apps.

STRENGTHEN YOUR WEAKEST LINKS

Address elements of the OWASP Mobile Top 10 Risks that are being neglected. Lack of binary code protection and lack of transport layer protection were the two most prevalent security risks identified.

MAKE SECURITY YOUR COMPETITIVE ADVANTAGE

Market the strength of security in your applications as a means to attract and retain customers. Security is increasingly becoming a determining factor in purchasing and usage decisions.

FOR APP USERS:

ONLY DOWNLOAD APPS FROM AUTHORIZED SOURCES

Most authorized app stores have some security protocols in place to help ensure applications can be trusted.

DON'T JAILBREAK OR ROOT YOUR DEVICES

Jailbreaking/rooting devices negates security measures that are designed to help protect you and your data.

DEMAND TRANSPARENCY OF OF YOUR APP'S SECURITY

Just like food nutrition labels, understand what risk you are "consuming" before downloading your apps. Become an advocate for certification and risk transparency.

Footnotes:
[1] Mi3 is a third-party independent application security company that interrogates mobile apps for malware threats, privacy risks, and data leaks.

[2] The Open Web Application Security Project (OWASP) Mobile Top 10 Risks identifies the most critical risks facing applications.

Sources:
[a] IBM Security / Ponemon study: The State of Mobile App Insecurity (February 2015)

For additional details & full report, visit Arxan.com

ARXAN