IoT Consumer Cybersecurity

In 2020, IoT hardware made up around a third of the total number of infected devices. (Forbes) However, at the same time some other surveys also suggest that consumers are willing to pay more for secure IoT devices.

CHALLENGES

Lack of security concerns:
Spying on private households through hacked cameras is now not only the prerogative of fictions.
The reality is that security is not implemented in many current Consumer IoT. IoT devices are typically attacked within five minutes of connecting to the internet.

Increased varied technologies:
Connected objects lead to the development of overlapped wide ecosystems boarding an important varieties of different technologies, which in turn, creates a higher number of entry points for potential cyber attacks.

Address the security at the right cost:
By definition, security requires a minimum of calculation power, and this has a cost. In order to reduce the cost, security must be approached with efficiency and expertise.

Certification:
It is hard for consumers to evaluate whether a device is secure against cyber attacks.
A higher level of consumer trust could be gained through union – wide certification.
Different security standards may be applied to assess the security of IoT devices.

OPPORTUNITIES

$1.1B The wearable devices market will be worth $1.1 billion by 2022

$142B The Consumer IoT market is on pace to reach 142 billion U.S. dollars by 2026, at a CAGR of 17% (Dataprot)

$58.7B The value of the global smart homes market was $58.7B in 2020 (Statista)

STUDIES HAVE SHOWN THAT CONSUMERS ARE WILLING TO PAY MORE FOR SECURE IOT DEVICES

7 out of 10
own an IoT device

3 out of 4
plan to purchase an IoT device in the next 12 months

Consumers want to own IoT devices, but they are deeply concerned about their security and privacy

81%
concerned about personal information being leaked

73%
concerned about hackers taking control of device and using it to commit crime

72%
concerned about hackers gaining access to personal information

71%
concerned about being monitored without their knowledge or consent

- Internet Society

HOW CAN *RED ALERT LABS* HELP MAKING YOUR JOURNEY MORE SECURE ?

We can train you

- Red Alert Labs provides Cybersecurity trainings and awareness campaigns for consumer IoT manufacturers, subjects as current market situation, incidents, threats and risks, regulation, standards and best practices are covered

We can support you

- To Meeting standards that you need
- In product development process to safe your time, money and resources
- During the full process of designing secure IoT devices to meet your security objectives

We can evaluate your product security

- Through customized security assessments and test campaigns in preparation for product approvals and against relevant standards
- Through gap assessment and design reviews for hardware, software, mobile apps and IoT backend platforms
- Through Vulnerability Analysis and Penetration Testing on all the Consumer IoT interfaces (Hardware, software, crypto algorithm and protocols, IT and cloud Infrastructure, governance risk and compliance, …)

We can accompany you in the certification process

- By assisting you to obtain the certification you are targeting
- By providing a conformity assessment program for consumer IoT that allows alignment of the risk exposure to an appropriate assurance level

WE MASTER *STANDARDS & REGULATIONS* THAT IMPACT CONSUMER IoT

- ETSI Cyber Security for Consumer Internet of Things – EN 303 645
- IoT Security Foundation – The IoT security compliance framework
- GSMA IoT Security Guidelines & Assessment
- NISTIR 8259A
- The UK IoT 'security by design' law (in progress)
- Eurosmart
- GDPR

✉ *contact@redalertlabs.com*
🌐 *www.redalertlabs.com*
in *Red Alert Labs*
@RedAlertLabs
Aflortville (Paris Area) 94140, France

RED ALERT LABS
IoT Security