WHY SHOULD I CARE ?

QSecure

RUNEsec

The ART of Penetration Testing

WHO WE ARE

Vasilis Sikkis | QSecure

Senior Penetration Tester

Vasilis is an information security professional with 5 years of experience in information security, risk management and penetration testing. Vasilis was the team captain of the Cyprus National ECSC team that competed in the European Cyber Security Challenge in 2017 and an active mentor ever since.

OSCP | eCPTX

Simon Loizides | RUNESEC

Hacker

Simon is a security practitioner with 6 years of experience in offensive security, namely penetration testing, security workshops and CTF challenge creation. Simon was one of the two coaches of the Cyprus National ECSC team that competed in the European Cyber Security Challenge in 2017 and an active mentor ever since.

OSCP

THE RISE OF THE REMOTE WORKFORCE

01

The coronavirus pandemic has forced global businesses to adopt to new ways of working and collaborating.

02

As a consequence, the demand for digital technology has skyrocketed.

03

Such rise of technology need has also become a much bigger and more lucrative target for cybercriminals.

2,145,013
phishing sites were registered by Google as of Jan 17, 2021. 27% increase over 12 months

Since the pandemic began, the FBI reported a

300%

increase in reported cybercrimes. (IMC Group)

Remote workers
have caused a security breach in 20% of organizations. (Malwarebytes)

THE STATE OF CYBER SECURITY IN CYPRUS

Our experience from Penetration Tests and Incident Investigations shows that compromised organizations do not announce their security breaches and hence:

- Other organizations in the same industry are not vigilant
- Threat level not publicly known and overall security in Cyprus doesn't increase
- Absence of a "criminal hacker" community worsens the security preparedness of Cyprus companies
- No legal action from clients and / or shareholders of compromised organizations lets ignorant / irresponsible C-level personnel get away with loose security controls

MOST COMMON CYBER ATTACKS IN CYPRUS

The same as in the rest of the world

1. Phishing with

- Malicious email attachments
- Fake change of bank a/c details

2. Exploitation of vulnerabilities or misconfigurations

- From websites / external facing systems

3. Insider threats

- Intentionally or not

What do they want? **MONEY** from:

- Ransom paid to recover encrypted data
- Extortion to prevent public release of stolen data
- Stolen cryptocurrency wallets
- Selling data to competitors
- The compromised organization directly or its clients

WHY YOU ?

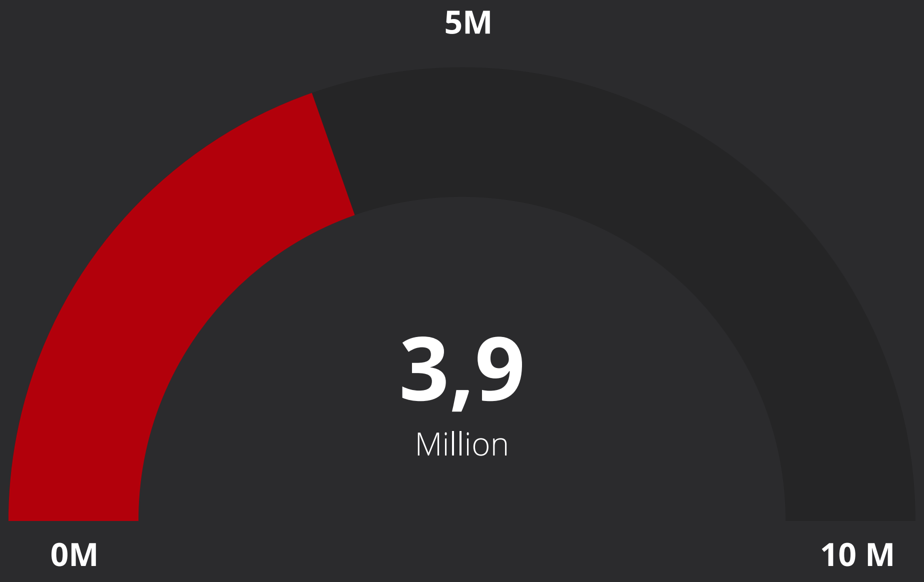
- Because you have access to your CLIENTS' data
- Because you might be easier to compromise than your clients.
- Because you aren’t aware of security best practices
- Because you don’t have time to apply security best practices
- Because you think you don't have the budget for security
- Because you think security can be solved by employing products (firewalls, antivirus etc)
- Because you think that you are not big enough to be a target and nobody will bother compromising you
- Because you think security is an IT problem, rather than a BUSINESS problem

LEGISTLATION AND FINES

Being compliant with standards (e.g., GDPR, ISO 27001, PCI DSS, etc.) doesn't mean you are protected

- GDPR has shaken things up a bit, but most organizations are compliant only on paper.
- Technical security measures are still lagging behind baseline security settings
- Fines issued based on GDPR will have slow impact on changing the overall culture in CY because the Office of the Commissioner can audit only a small number of companies annually
- Attackers don't care if you are XYZ compliant.

AVERAGE COST OF A SECURITY BREACH



On average, all organizations globally with the selected cost factors will incur the cost above for a data breach
Source: IBM

QUESTIONS

WHAT IS THE MOST EFFICENT WAY TO PROTECT YOURSELF?

With a PENETRATION TEST

- It’s the most cost-effective solution
- Assess your overall security posture
- Identify a spectrum of vulnerabilities
- Show the impact of exploiting those vulnerabilities (!)

Don't fall into the trap of acquiring more security solutions and blowing through your budget without assessing your overall security posture first.

AND NOW WHAT?

What follows a Penetration Test?

- A detailed report describing vulnerabilities found, their impact and recommended mitigations
  - 70-100% of mitigations are fixable without any new hardware / software
- Implement security vetting in your procurement process (ask for Penetration Test reports)
  - Has your IT provider ever done a Penetration Test on their systems? If not, they're a weakness into your organization
  - Has the vendor of your new application tested their product? If not, it could be a weakness into your organization.
- Implement security clauses in your service agreements with vendors / IT partners
  - Their job is to fix identified security weaknesses (hopefully at no extra cost)
  - Our job is to find the security weaknesses and help IT fix them
- Your personnel are your strongest asset; trust and support them

Information Security 101

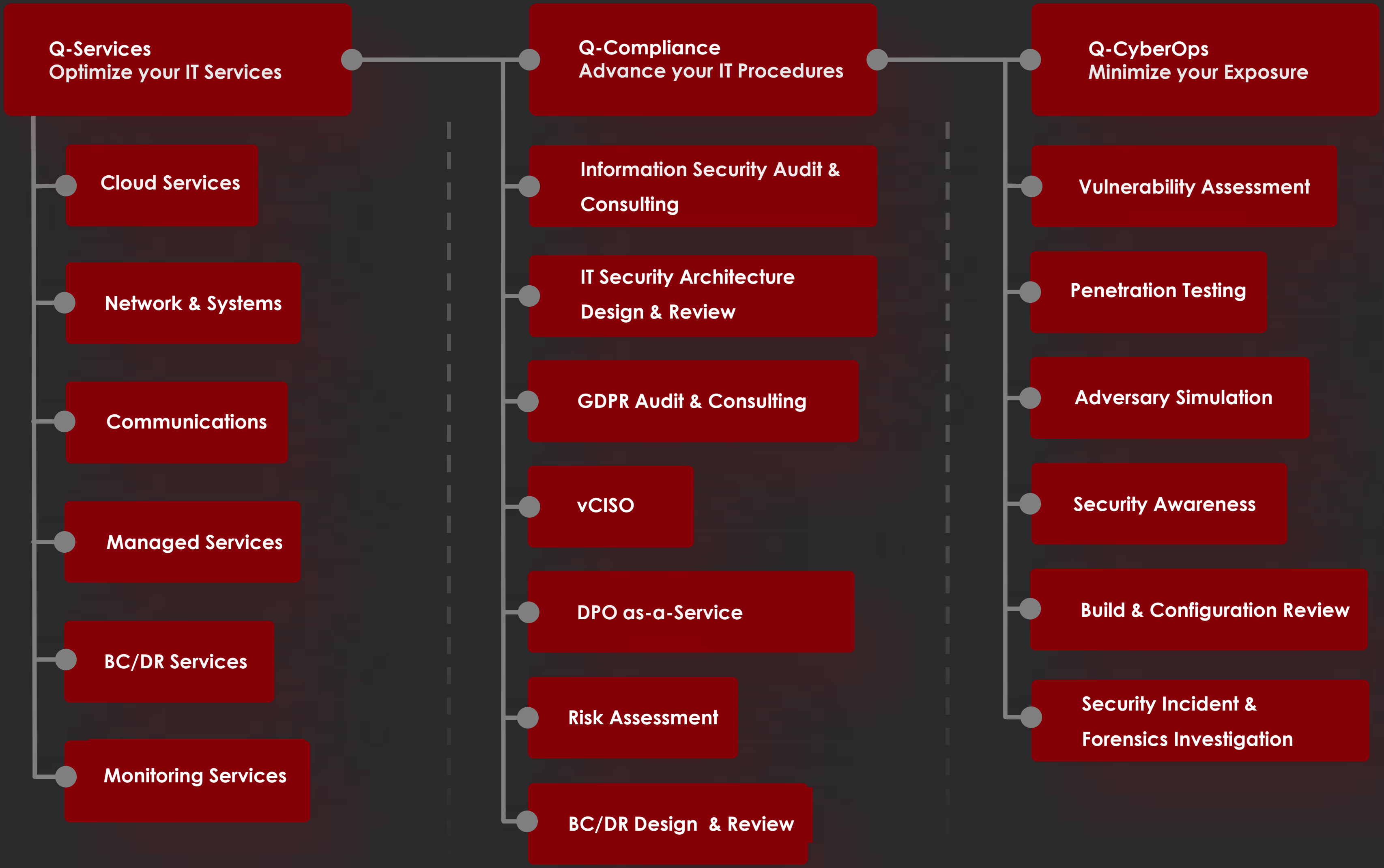
- Keep your systems and applications up-to-date
  - Apply security patches regularly
- Harden the security configuration of your systems
  - Change default passwords (we find these all the time)
  - Disable insecure, legacy network protocols
- Design your systems with security in mind and employ security best practices
  - Segment your internal network if it's big
  - Don't expose unnecessary services to the public Internet (configure a VPN if you need to)
  - Use two-factor authentication for publicly accessible services (e.g. email)
- Educate your employees on cybersecurity threats
  - Passwords, passwords and passwords (!)
  - Phishing threats
- Vet your vendors / partners
- Microsoft Defender (antivirus) and Windows Firewall are just fine if you are not doing the above

AND REMEMBER

ONE FINAL TIME!

"I think we're named after computer passwords."

OUR SERVICE LINES | QSECURE



Q-Services
Optimize your IT Services

- Cloud Services
- Network & Systems
- Communications
- Managed Services
- BC/DR Services
- Monitoring Services

Q-Compliance
Advance your IT Procedures

- Information Security Audit & Consulting
- IT Security Architecture Design & Review
- GDPR Audit & Consulting
- vCISO
- DPO as-a-Service
- Risk Assessment
- BC/DR Design & Review

Q-CyberOps
Minimize your Exposure

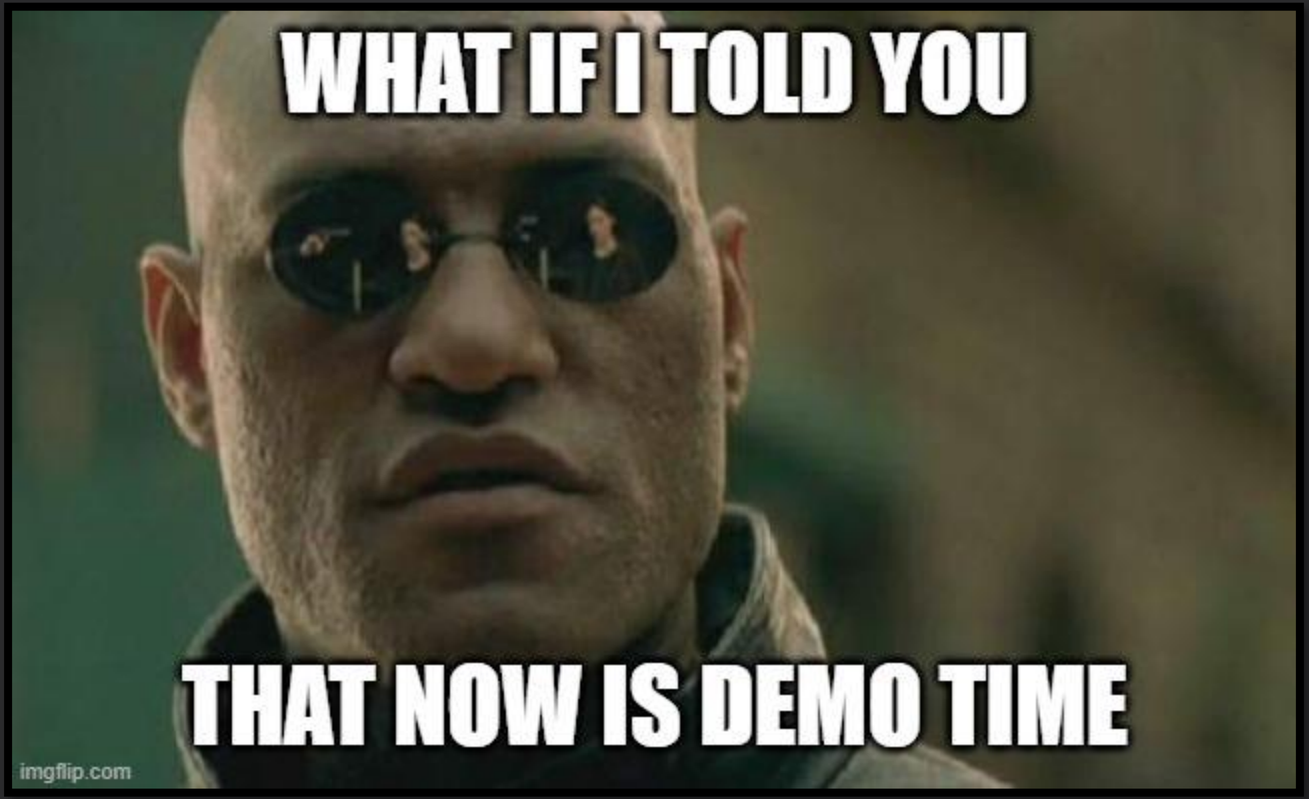
- Vulnerability Assessment
- Penetration Testing
- Adversary Simulation
- Security Awareness
- Build & Configuration Review
- Security Incident & Forensics Investigation

https://www.qsecure.com.cy

OUR SERVICE LINES | RUNESEC

- Vulnerability Assessments
- Penetration Testing
- Security Workshops
- Software Development Advisory
- CTF Challenge Creation

https://www.runesec.com.cy


WHAT IF I TOLD YOU
THAT NOW IS DEMO TIME
imgflip.com

THANK YOU!

Questions?