Building an Effective Security Strategy

6/4/2016

Information Security

Nikitas Kladakis
Information Security Director
CCSE, IBM Certified,MSCE+I

Agenda

- Company Profile
- Threat Environment
- Five Steps for Stronger Security

© netbull, 2016

Company Profile

- **Netbull** founded in 2013 from executives of **BULL** Greece with experience in large IT projects of the public and private sectors, as a leading System Integrator and Value Added Solutions Provider in the field of information security

- **Netbull** has local presence in Athens (Greece) and holds ISO 9001:2008 and ISO 27001:2013 Certifications

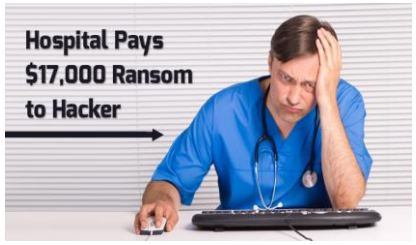
- Our Security Offer:
  - Security Services
  - Security Solutions
  - Managed Security Services
  - WAF as a Service

ISO 27001 BUREAU VERITAS Certification

ISO 9001 BUREAU VERITAS Certification

© netbull, 2016

Threat Environment



(Why Traditional Security is not Enough?)

© netbull, 2016

The New Environment: Internet of Things

© netbull, 2016

Ransomware

HOLLYWOOD PRESBYTERIAN MEDICAL CENTER

February 17, 2016

I am writing to talk to you about the recent cyber incident which temporarily affected the operation of our enterprise-wide hospital information system.

It is important to note that this incident did not affect the delivery and quality of the excellent patient care you expect and receive from Hollywood Presbyterian Medical Center ("HPMC"). Patient care has not been compromised in any way. Further, we have no evidence at this time that any patient or employee information was subject to unauthorized access.

A recent study of U.S. hospitals found that 52 percent were infected with malicious software.

http://fortune.com/2016/04/01/u-s-hospitals-face-growing-ransomware-threat/

© netbull, 2016

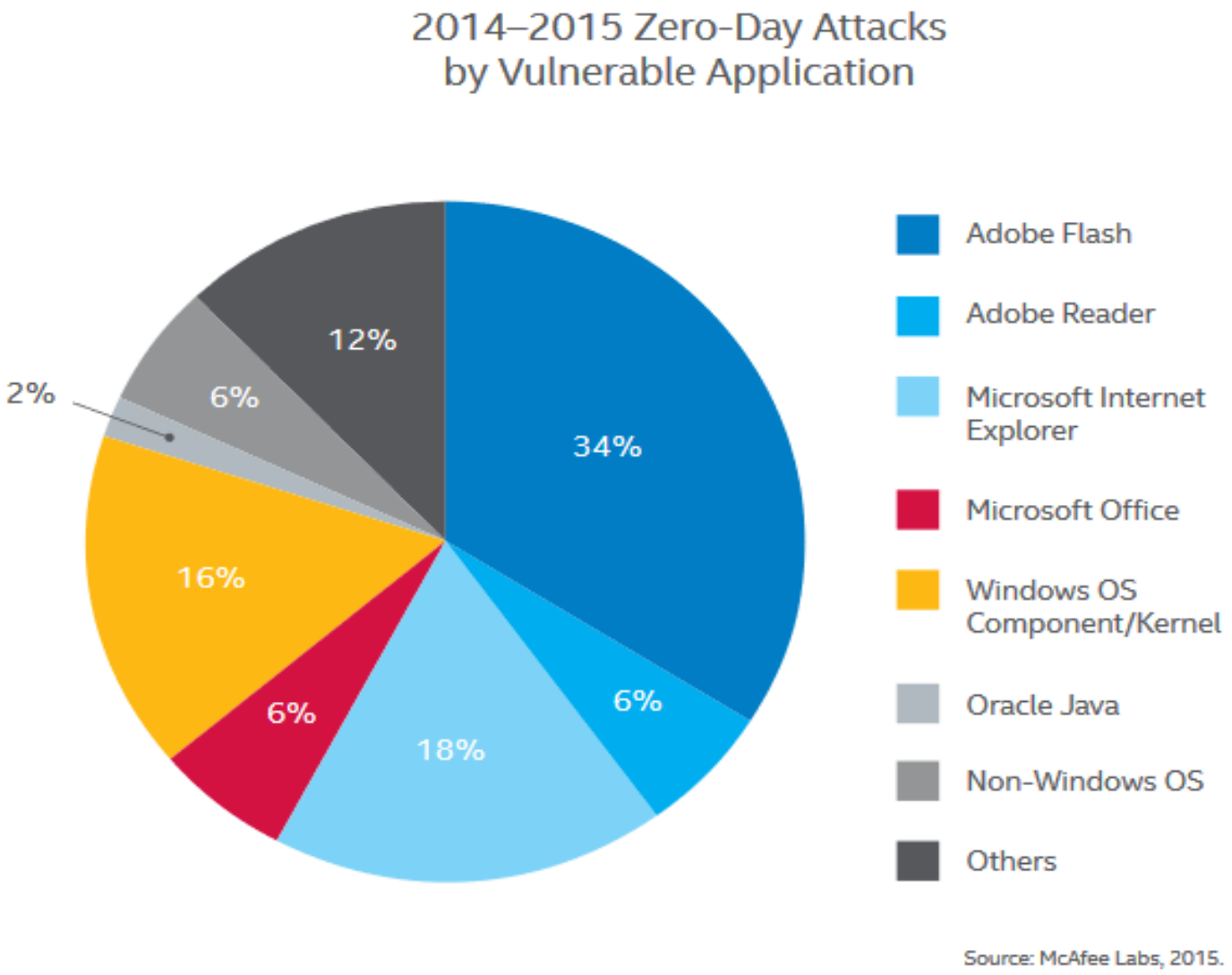
Hacktivism

Source: "Anonymous at Scientology in Los Angeles" by Vincent Diamante. Originally posted to Flickr as Anonymous at Scientology in Los Angeles.

Licensed under CC BY-SA 2.0 via Commons—https://commons.wikimedia.org/wiki/File:Anonymous_at_Scientology_in_Los_Angeles.jpg#/media/File:Anonymous_at_Scientology_in_Los_Angeles.jpg

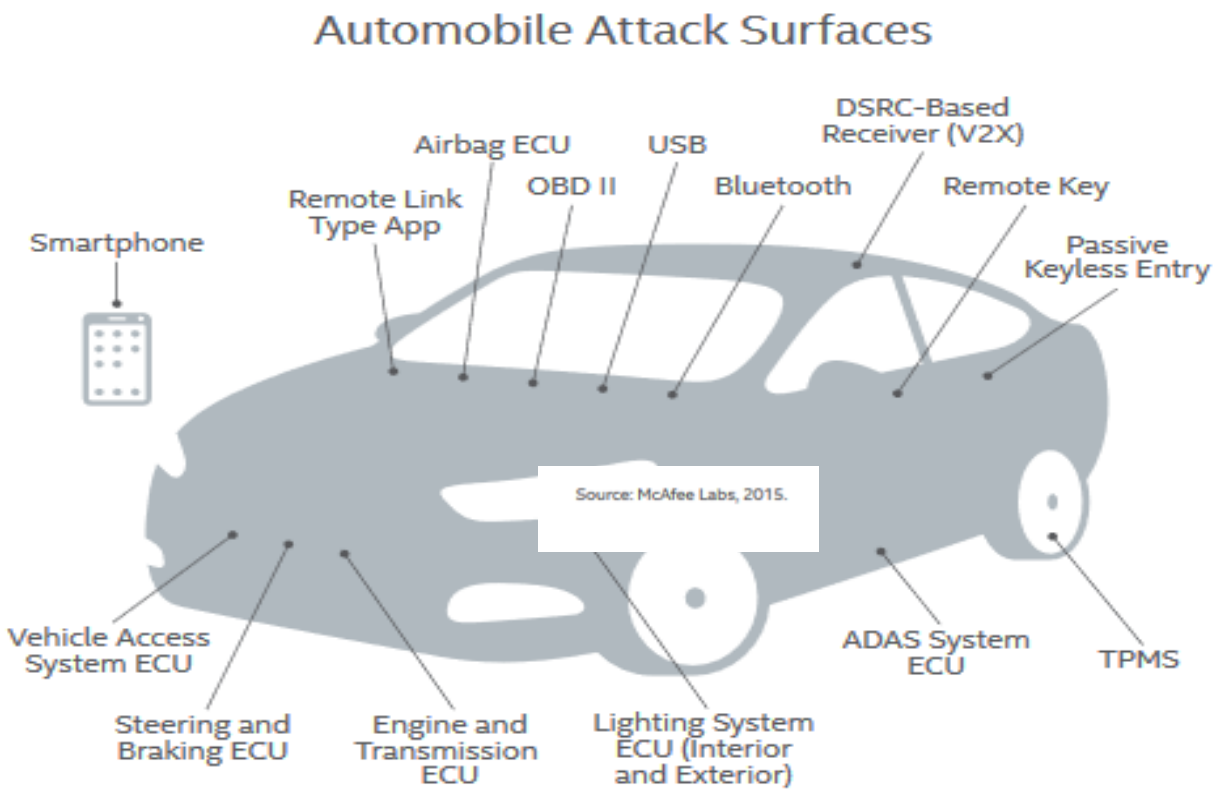
© netbull, 2016

Zero Day Vulnerabilities



© netbull, 2016

Automobile Attack Surfaces



Fifteen of the most hackable and exposed attack surfaces, including several electronic control units, on a next-generation car.

According to the Business Insider "The Connected-Car Report," there will be 220 million connected cars on the road by 2020.

Source: McAfee Labs, 2015.

© netbull, 2016

Wearable Attack Surfaces

Wearables Attack Surfaces

- Operating system kernel
- Networking software/WiFi
- User interface
- Memory
- Local files and storage system
- Access control/security software

- Cloud virtual machine and control apps
- Web app
- Memory
- Local files and storage system
- Access control/security software

Source: McAfee Labs, 2015.

© netbull, 2016

Security Predictions for 2016

1. Sniper' and 'shotgun' malware
2. More mobile threats
3. More businesses will turn to advanced threat prevention
4. Critical infrastructures will be highly targeted
5. IoT and smart devices are still at risk
6. Wearables won't be safe, either
7. Trains, planes, and automobiles
8. Real security for virtual environments
9. New environments will bring new threats
10. Organizations will look to security consolidation

http://blog.checkpoint.com/2015/12/01/check-points-security-predictions-for-2016

© netbull, 2016

Five Steps
For Stronger Security

(How to Build an Effective Security Strategy)

© netbull, 2016

Step 1 – Risk Assessment

© netbull, 2016

Risk Assessment

- Assets
- Vulnerabilities
- Threats
- Risks

© netbull, 2016

Step 2 – Choose a Security Strategic Plan

© netbull, 2016

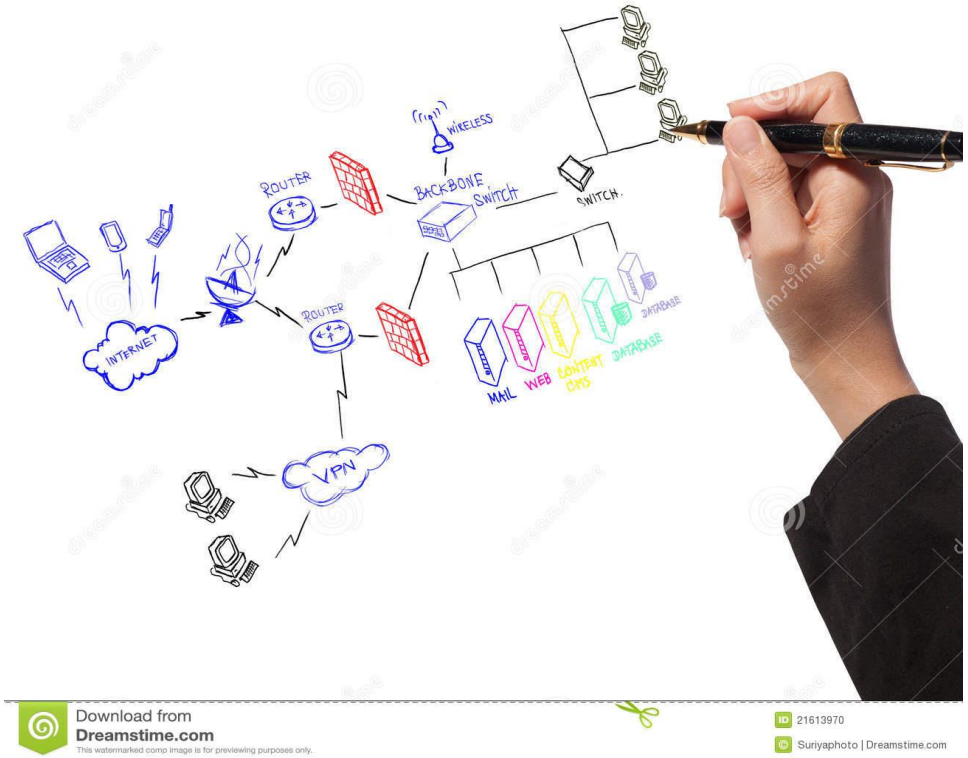
Security Architecture

nSA: netbull 3D* Security Architecture

© netbull, 2016

Security Plan

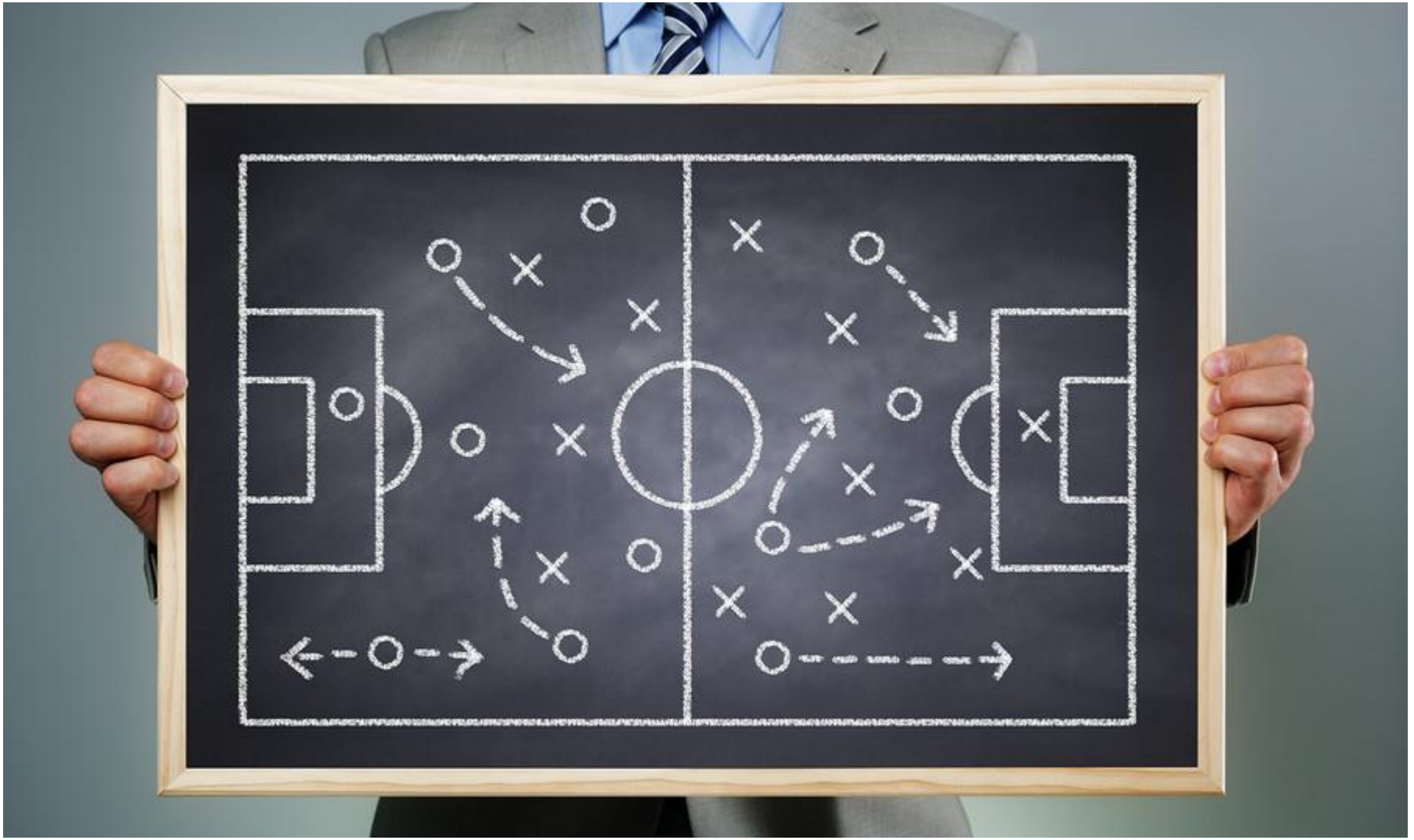
- Organizational Controls
- Management Controls
- Technological Controls



Download from
Dreamstime.com
This watermarked comp image is for previewing purposes only.
ID 21613970
Suriyaphoto | Dreamstime.com

© netbull, 2016

Step 3–Implementation of the Security Strategic Plan



© netbull, 2016

Implementation of the Security Strategic Plan

- Define Security Roles and Responsibilities
- Develop Policies and Procedures
- Implement necessary technical controls
- Implement security awareness and training across the entire staff

© netbull, 2016

Step 4 – Incident Monitor

© netbull, 2016

Incident Monitor

- Real-time 24x7x365 analysis and response to known and emerging threats

- Integration with any security device or critical information asset

- Automated event correlation

© netbull, 2016

Step 5 – Incident Management Plan

© netbull, 2016

Prepared for ...

- Investigation and Analysis
- Classification
- System Recovery
- Business Continuity
- Follow up

© netbull, 2016

For further information

Visit our website: www.netbull.gr

© netbull, 2016