學校網絡安全漏洞的評估分享，管理挑戰及趨勢

香港電訊有限公司
商業客戶業務總處
潘震宇先生
13th Jan, 2020
Agenda

1. Introduction
2. Assessment Result Sharing and Insight
3. Challenges in Security Management
5. Q &A
Introduction

School IT Security Risk Assessment

Objectives

- Create awareness - Privacy issues
- Identify vulnerabilities in local primary & secondary schools
- Set the standard (baseline) for the industry
- Vendor to provide service - Qualified security experts should be appointed for security risk assessment
Web vulnerability assessment lifecycle

- Information Gathering
- Vulnerability Analysis
- Manual Review
- Report and Recommendations
HKT Web Vulnerability Assessment Service is performed by a group of security certified engineers.
Result Highlights

- ~50 Websites
  Internet-facing application of 20 schools

- 150+ Hours of Scanning
  By using different Risk Assessment Tools and manual testing/review

- 110+ Critical Vulnerabilities
17% of vulnerabilities are Critical / High Vulnerabilities.
Among the ~50 scanned systems...

39% Code (SQL) Injection
Allow an attacker to compromise the application, access or modify data, or exploit latent vulnerabilities in the underlying database.

27% Cross-site Scripting (XSS)
The attacker’s hostile data can trick the interpreter into executing unintended commands or accessing data without proper authorization.

63% Using Outdated Components with Known Vulnerabilities
- SSL/TLS version
- OS version
- PHP version
- Apache version
...etc
- Data Leakage / Loss
- Content Defacement
- Malicious code injection
- Malware / Ransomware Infection
- Black Listing ↔ SCHOOL OPERATION / REPUTATION
Challenges in Security Management

10+ years ago

IT Support
Challenges in Security Management

More User Touch Point
More System
More Data (More Security Risk)

IT Support

Nowadays
Enterprises need to keep investing in Cyber Security

Success factors that can strengthen your organization’s cybersecurity posture in the next three years

- Improvement in technologies
- Improvement in staffing
- Increase in funding
- Cyber intelligence improvements
- Improvement in threat sharing
- Reduction in the compliance burden
- Ability to minimize employee...
- Reduction in complexity
- Increase in C-level support
- Cybersecurity leadership
- Other

Ponemon Institute Research Report, 2018

0% 20% 40% 60%
Trends in Security Management

How to Survive in the challenging Security Management?

You CANNOT do it all by yourself, find a TRUSTED PARTNER for Security Management
“Security-Centric” - Security Management Everywhere

Potential Security Threat is everywhere!!

Service Gateways

Internet Service Provider

Perimeter

Core Networking

End Point Devices/BYOD

INTRUSION

School Wi-Fi service

School core network

BYOD Devices

School Devices

DDoS / Malicious Website

ISP

DoS / Intrusion

School Firewall

RANSOMWARE / Email SPAM / Email Spoofing

VIRUS / MALWARE

User Remote Access

User Remote Access
“Security-Centric” - Security Management Everywhere

Multi-Dimension Security Protection

- Service Gateways
- Internet Service Provider
  - Cloud-Based Firewall / Web Filtering
  - User Remote Access
- Perimeter
  - School Firewall
  - UTM Firewall
- Core Networking
  - School Wi-Fi service
  - School core network
  - Email Security / Application Server EDR
- End Point Devices/BYOD
  - BYOD Devices
  - School Devices
  - Cloud-Based Firewall / Web Filtering
  - User Remote Access

NGAV
Comprehensive Managed Security Service

1. Centralized Security Log collection and monitoring
2. Automation of security alert and incident recording
3. Remote support for incident recording and assist
Key components on Security Management

Ongoing Support

People

Technology

Process

Secure Connectivity

DDoS Protection

HKT Internet Platform

HKT Private Network

HKT School HelpDesk / Security Operation Center

Secure On-Premises Solution

System Security

Application Control

Network Security

Endgame Protection

Customer Premises

HKT Internet Platform

HKT Private Network
## Security Operation Center

- Security Expert
- Security Intelligence
- Security Management

<table>
<thead>
<tr>
<th>Tier 1</th>
<th>Tier 2</th>
<th>Tier 3</th>
</tr>
</thead>
<tbody>
<tr>
<td>SOC Manager</td>
<td>Tier 2</td>
<td>Tier 3</td>
</tr>
</tbody>
</table>

Tools and Practice
Occurred on 12-May-2017 (Friday night)

Take action to **disable related firewall TCP ports (139 & 445)** in **ALL** school wifi circuits

Completed all school wifi circuits (400+) on 15-May-2017 (Monday)

Informed schools that HKT already take action to block the TCP ports via **Phone & Email**

Prepare user guide / preventive actions and sent to schools for **them to take action on school’s ITED network**
Key Takeaways

- Security Risk will keep **Evolving**

- **Periodic** Security Risk Assessment is important

- You **Cannot** do it all by yourself

- Find a **Trusted Partner** for security management
Any Questions?
Follow HKT Enterprise Solutions on LinkedIn & Facebook

Follow us on

LinkedIn

HKT

Facebook

FOLLOW US ON FACEBOOK
Thank You