SMART CITY CATALYST
THE URBAN INNOVATOR

CYBER-PHYSICAL SECURITY

juni 3

2015

Smart City technologies are being deployed across the globe in energy systems, transport, water, and health sectors, but how safe are the systems and networks from theft, intrusion, remote access, and malicious attacks? With the rise of commercial and state-sponsored cyber warfare and well-organized criminal gangs, cities need to step up their game in cyber-physical security.

CYBER-PHYSICAL SECURITY CHECK LIST

IT and Cyber-Physical Security Governance	Proactive policy/action
Does your organization conduct regular reviews of known and potential vulnerabilities?	A reliable overview of your system is key when a system has been breached. Knowing what systems are critical to maintain service levels helps to ensure continued operations.
Does your organization have a risk mitigation strategy?	The lack of a formal cyber-physical risk mitigation/management strategy is common in many governmental, energy, transport, and other utility sectors
Does your organization conduct live exercises to test your system?	Governments and utilities infrequently conduct live penetration tests of their systems, but such exercises (white hat, grey hat, or black hat) are important to find vulnerabilities before someone else does.
Does your organization outsource cyber-security?	If so how they are affiliated and what do they have access to? If not, how often do you do penetration test (min. of 4 tests a year must be done using known exploits).
Does your organization have multiple failsafe backups for critical system failure?	Even short-term disruption of the most vulnerable urban systems (energy, transport, water, etc.) can lead to cascading chains of failure, leading to potential loss of life, economic losses, and political backlash. Organizations need to be prepared for digital systems to fail and have adequate analog systems on stand-by.
How many third parties have access to your organization's systems?	Hackers frequently use third-party access, bypassing stronger security protocols. Knowing who has access to what systems is a must.
How many databases does your organization use?	Many large municipal and state organizations do not have a basic overview of how many and what type of databases are used. Mapping these is a critical first step in order to see the overall architecture of the system
Does your organization conduct regular security training for IT users	Password re-use, opening malware in email files, and device management procedures are frequently the cause of significant breaches of systems and data. Organizations that routinely train their users have higher levels of security compliance than those who do not.

Does your organization have an identity management system in place?	While single sign-on systems are user friendly, they can introduce the same vulnerability as frequent re-use of simple passwords.
Does your organization have a BYOD (Bring Your Own Device) policy?	BYOD policies introduce an entirely new attack surface, since most organizations do not adequately screen for apps installed by users for either work or personal reasons

IT and Operations Department	Proactive policy/action
Does your organization rely on firewalls, intrusion protection systems, anti-virus, and Web gateways for cyber security?	The majority of attacks today are multi-vector, multi-stage types using a variety of tools including worms, malware, zero-day exploits, and known system vulnerabilities to bypass traditional security tools.
Does your organization employ an incident response system to counter malicious attacks?	The average time between a malicious breach and target response is over 240 days, leaving plenty of time to extract whatever data the attackers require. Dynamic real time network traffic analysis and automated threat detection is required to counter more sophisticated techniques.
How frequently does your organization patch software?	In most large organizations, large numbers of legacy software systems means that regular software patches often require significant downtime and custom coding, and as result software is left unpatched even for critical security issues.
What type of malware detection and email scanning systems does your organization use?	Most firewalls and malware detection systems are incapable of catching sophisticated attacks. Reliance on outside IT contractors has shown to fail routinely.
Does your organization possess the capability to detect firmware hacks?	An increasing number of state and non-state actors are using sophisticated zero-day exploits (Flame, Regin, EquationLaser, EquationDrug, and GrayFish) to infect firmware, bypassing software anti-virus and firewall protection
Does your organization use Microsoft Office suite?	A large percentage of malware infections occur through Microsoft products, with custom exploits available for as little as €1500
Does your organization use Java?	Java products contain a number of vulnerabilities that are frequently exploited by malicious attackers to gain entry into sensitive databases

Which browsers are used in your organization?	Microsoft Internet Explorer (particularly older versions) have a number of known security holes that allow for malicious attacks.
Do you use Adobe products?	Many malicious attacks use known vulnerabilities in common Adobe software, particularly Adobe Reader and Flash
Does your organization rely on air gaps (no network connectivity) to secure critical infrastructure?	Air gaps no longer provide protection from malicious attacks. USB sticks with malware use radio signals to infect devices and pull information onto the Internet
Does your organization or IT outsourcing company routinely update their security systems using the Common Vulnerability and Exposure CVE) database?	The CVE database is a global central repository of known software vulnerabilities and exploits, and should be frequently checked to ensure your organizations' systems are protected against known threats.

Personal data protection	**Proactive policy/action**
Does your organization salt and hash sensitive data?	Most organizations do not routinely salt and hash sensitive data, including passwords, financial, and health information. Plain text storage of sensitive data makes your organization an easy target for cyber-criminals or state-sponsored hackers
What type of encryption standard does your organization use?	Free programs like oclHashcat and Jack the Ripper combined with easily available rainbow tables of known compromised passwords makes cracking software like bcrypt and SHA1/SHA2 easy. PBKDF2 is the preferred crypto option.
Is your organization compliant with the new EU data protection directive?	New EU data protection laws will introduce harsh penalties for privacy breaches of personal data. Many Smart City initiatives rely on tracking and storing personal data which may become illegal under the new directive.

If you would like to know more about Smart Cities Governance/planning and cyber-physical security feel free to contact us.

PATRICK DRISCOLL
PATRICK@SCC-EU.DK

MARTIN TOM-PETERSEN
MARTIN@SCC-EU.DK