

CYBERSECURITY CANNOT BE AN AFTERTHOUGHT
IN OUR SMART CITY JOURNEY



SMART CITIES

Logicom
Solutions

Efficient public services

Reduce energy consumption

Online services to citizens

What about Cybersecurity?

1

Incidents against cities in the world

Presentation of real incidents affecting thousands of people

2

Targets, risks and key challenges

What can be targeted and our key challenges

3

Planning and way forward

How can smart cities be protected against cyberattacks





FLORIDA, NEVADA, CALIFORNIA

Water Treatment Plan: Different types of attacks, including the change of chemical levels used to treat water. In

COSTA RICA

Tax Collection System: Attackers targeted the Costa Rican Ministry of Finance. The President of Costa Rica declared a national emergency. Hackers asked for 20mlns in ransom.

UNITED KINGDOM

Port of London Authority: A DDoS attack targeted the Port of London Authority, forcing its website to go offline. A group linked to Iran took responsibility for the hack.

Attacks
r-traffic
ircrafts.
multiple
ed 3
d 30
than
lectricity.

**We have
seen this
happening**

**IN THE
REAL-WORLD**



THE THREAT LANDSCAPE IS CHANGING



1



DIFFERENT THREAT ACTORS

The threat actors are changing to online fraudsters

2



ATTACK SURFACE IS CHANGING

New services and channels are being introduced which can be targeted

3



NO PHYSICAL CONSTRAINTS

A city can be targeted from anywhere, from everyone.

4



AGAINST WELL ORGANIZED GROUPS

It's not only individuals. Sophisticated and well organized groups are the major threat.



THE MOST INFAMOUS HACKING GROUPS



LAZARUS HACKING GROUP



SILENCE HACKING GROUP



CODOSO HACKING GROUP



CARBANAK HACKING GROUP



**MORE THAN 100
HACKING GROUPS**



BUSINESS CONSULTING SERVICES

Smart City Services that can be targeted



SMART TRAFFIC CONTROL

Security review of the newly developed banking systems and infrastructure.



CCTVs - CAMERAS

Traffic and surveillance cameras can allow attackers to spy or make cities blind.



MANAGEMENT SYSTEMS

Attacks targeting the different internal systems to cause impact on the operations.



SMART GRID

Attacks against the smart grid can result in a black-out.



SENSORS

To send fake data and affect how automated decisions are made (e.g. Raise alerts, panic).



STREET LIGHTING

Compromise the street lighting system to take control and turn on-off the lights.



SMART TRANSPORTATION

Display incorrect information, cause delays and overcrowding.



SOCIAL MEDIA

Comprised social media accounts and posting of fake news or notifications to cause confusion.



PUBLIC DATA

The crown jewels of every organization. Exfiltrate sensitive data is always a key objective.

KEY CHALLENGES

to secure smart cities' environment



1



INADEQUATE SECURITY CONTROLS

Weaknesses in the design or the implementation of controls.

2



LACK OF CYBERSEC EXPERTS

Worldwide, there are more than 2mln positions of cybersecurity experts that are unfulfilled.

3



LEGACY / OUTDATED SYSTEMS

Outdated or legacy systems is one of the most important weaknesses that can result in an incident.

4



EXTENDED ATTACK SURFACE

To safeguard the expanding attack surface, a solid and structured approach is needed.

5



PUBLIC SECTOR CHALLENGES

Procedures that require time may be restrict organizations from responding promptly.





Areas that will be impacted

What are the consequences in the event that we do not secure our cities?



NATIONAL
SECURITY



NATIONAL
ECONOMY



SOCIAL
WELLBEING



HEALTH AND
SAFETY



ENVIRONMENT

1

PERFORM RISK ASSESSMENTS

Assess your risks, identify threats and evaluate the effectiveness of your controls and prepare your risk treatment plan.

2

CONDUCT PENETRATION TESTS

Simulate hackers' activities to identify the possible entry points to your environment or services.

3

INCIDENT RESPONSE PLANS

Be prepared to respond to an incident and to recover the operations in the event of a successful cyberattack.

4

CONTINUOUS SECURITY AWARENESS

Run a continuous security awareness programme. Human factor is still the weakest link in the security chain.



CHARIS FLORIDES
CISSP, OSCP, MSc in InfoSec



Division Head,
Business Consulting Services
Logicom Solutions



Board Member
ISC2 Cyprus Chapter



email address
c.florides@logicom.net



Linkedin Profile
charis.florides

