Cyber Israel
Prime Minister's Office
National Cyber Directorate

Best Practice

Reducing cyber security risks in video surveillance cameras

April 2018

Guidelines

Cyber Israel
Prime Minister's Office
National Cyber Directorate

Reducing Cyber Security Risks in Video Surveillance Cameras

April 2018

This guideline was written by the Prime Minister's Office - Israel National Cyber Directorate in the interest of public welfare and provides recommendations to all organizations and entities in the State of Israel with the aim of enhancing their cyber-resilience capacities. It is intended for use by the general public, organizations, security and low-voltage consultants, security officers, infrastructure specialists and implementers as a guide to best practice, and provides recommendations for reducing cyber risks arising from the use of video surveillance cameras. Organizations are strongly encouraged to conduct a risk analysis and will be able to develop a robust protection plan based on the recommendations provided herein. Feedback on the content of this document should be sent by email to: **tora@cyber.gov.il**.

Table of Contents

Introduction and purpose of this document

The increasing dependency on the cyber realm (cyber domain) is the result of technological progress, linkage and global connection to the network. The technological capabilities and threats developing in the cyber realm do not distinguish between organizations and individuals. Consequently, both parties may become a target for attack. The primary purpose of this guidelines document is to improve the national and organizational resilience as well as privacy and personal safety.

The use of sensors, **video surveillance cameras** with Wi-Fi capabilities, and cameras containing IoT (Internet of Things) components has increased in recent years. IoT communication is a form of sophisticated communication between objects that are capable of collecting and exchanging information. Such technology enables Internet connectivity, information sharing between components and reception of updates at Any Time and Any Place. In spite of the tremendous advantages conferred by the use of IoT components, many different studies have revealed **inherent** security vulnerabilities in IoT components and hostile takeover processes.[1] Because this technology facilitates automation and inter-component communication, it creates a security risk and an opportunity for attackers to intervene in and manipulate both inter-component communication and the system as a whole.

Examples of IoT systems

Use of IoT-based technologies without adequate security definitions makes cameras a target for attacks which may result in data theft, data disruption, impersonation, blocking, etc[2]. Attack methods can also involve searching for video surveillance cameras by querying the manufacturer's name and default passwords. Other possibilities **including camera IP address exploitation, specific attacks to create loads (deny service), or use the cameras in an unauthorized or unlawful operation.**

The wide deployment of cameras in organizational and private environments can increase security risks and the risk of unauthorized entry into the security systems, including attacker intervention in software update processes (MITM), etc.[3]

This guideline has been adapted to the Israeli economy and includes recommendations for reducing cyber risks arising from the use of cameras. It was written, among other

1 See the study by Eyal Ronen, PhD student at Prof. Shamir's laboratory, Achi-Or Weingarten, MSc student at the Weizmann Institute, and Colin O'Flynn, "Hostile takeover of the IoT network of the Weizmann Institute" - https:// eprint. iacr.org/2016/1047.pdf.

2 Security Issues in the Internet of Things (IoT): A Comprehensive Study - (IJACSA) International Journal of Advanced Computer Science and Applications, Vol.8, No.6, 2017 (Risks incidence table - page 388).

3 http://www.newshub.co.nz/home/world/2017/02/hackers-hacked-washington-cameras-before-trump-s-inauguration.html.

considerations, with reference to lesson learned from history cyber-attacks that was used against cameras.

1. Pre-acquisition considerations

1.1 The rationale of this guidelines document is based on the known information security model set out by the CIA:

- **Data Confidentiality –** as part of **covertness** and prevention of unauthorized exposure of information.
- **Data Integrity –** Preventing unwanted data modification, falsification or destruction and ensuring the data remains authentic and unaltered by any hostile party.
- **Availability –** ensuring that the data remains accessible at all times.

1.2 In secure design, to reduce the security risks arising from the use of video surveillance cameras, the following scenarios should be considered:

1.2.1 Risks resulting from the use of IoT components.

1.2.2 Exploitation of camera infrastructure at the terminals for penetration into the organization's computer systems. Like any other software-based computer component, cameras may contain bugs, gaps, back doors and "opportunities" that can be exploited. These threats are significant as they provide stepping stones for attackers to steal commercial information, damage databases, implant Trojan horses and hostile codes for future attacks, etc. In this context, there is also a risk that the cameras and sensor infrastructure could be used to execute Denial of Service attacks (DDOS).

1.2.3 Intervention (MITM – Man in the Middle) for unauthorized viewing of data - Accessing the systems, taking control or listening (MITM) and viewing of image outputs.

1.2.4 Online attacks to shut down a system, prevent access to it, or execute a ransomware attack – Hostile takeover and forced entry to shut down the operation of the video surveillance cameras. In many incidents, attackers took control of the cameras, shut them down or changed the access password. In other cases, ransomware attacks were carried out on cameras.[4] On still other occasions, attackers disrupted the video surveillance cameras operation in order to create an opportunity and a time for physical break-in.

1.2.5 Information manipulation – An unsecured security system allows an attacker to manipulate and alter video traffic information unbeknownst to the system's operators.

1.2.6 Tampering with or deleting recordings – Altering or erasing recordings through unauthorized access, altering images, etc.

1.3 This guideline focuses on attacks on cameras at terminals as well as on the communication medium (between the cameras and the computers). The document is based on the assumption that sufficient resources have been invested in minimizing cyber risks to the existing servers and organizational infrastructure interfaces (in accordance with the organization's cyber defense doctrine)**. Therefore, this guideline does not deal with the physical characteristics of a camera array or how to deploy and install all the equipment in this system**.[5]

---

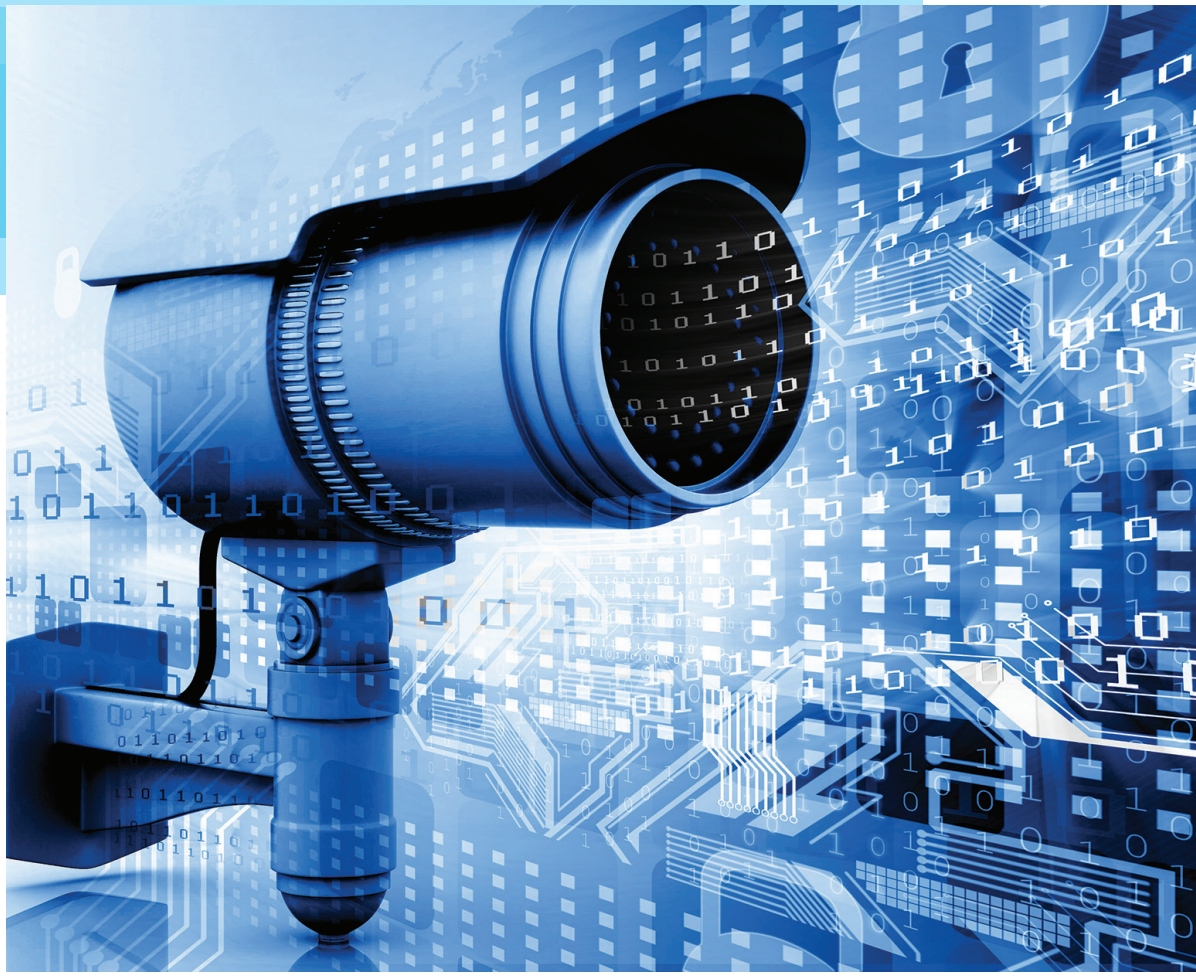
4 Malware attack for money extortion (Ransomware)

5 https://www.gov.il/he/Departments/Guides/cyber_security_methodology_for_organizations_test

Document target audience

This guideline is intended for private, public, and government organizations that intend to securely implement or integrate cameras, with the aim of reducing cyber risks arising from the use of video surveillance cameras. The subject requires appropriate consideration and preparation in order to ensure the safety and privacy of users and citizens while reducing cyber risks as much as possible.

The document provides recommendations and key points for consideration during the purchase, installation and setup phases and/or for the reduction of cyber risks in existing and active cameras. As such, it can serve as a security guideline for, among other things, system equipment and video surveillance camera vendors, security and low-voltage consultants and infrastructure personnel.



Technological threats to cameras - background

Video surveillance cameras are vulnerable to cyber threats **that may lead** to information security incidents, including information leaks and breaches of privacy. Among other things, the stimulus and attractiveness of the attack are due to the attacker's desire to access sensitive and/or private information (images, recordings, etc.), or to exploit security systems in general and video surveillance cameras in particular to gather intelligence before an operation.

Technological development leads to innovation and the use of video surveillance cameras for various purposes, including their incorporation into complex platforms such as the ones used to run smart cities, which are based on advanced computer systems and information and communication technologies. When conducting risk management relating to these uses, it should be remembered that **cameras can be used as a bridgehead from additional attacks against the organization computer networks.** Conversely, cameras can also be attacked via platforms and other network components based on smart city technology.

Most attacks rely on attacking password mechanisms (by means of default passwords, administrator passwords and password guessing), link exploitation (including IoT subjects) and unsecured or unencrypted channels for interception and listening.

Reducing cyber security risks in video surveillance cameras

1. Pre-acquisition considerations

1.1 It is preferable to acquire systems that are not IoT-based and do not include built-in, standalone communications components such as modems, wireless transmitters, etc.

1.2 Alternatively, **hardening** this hardware or software should be considered (preferably in coordination with and with the assistance of the manufacturer).

1.3 It is preferable to avoid installing software products that are not provided by the camera's manufacturer. If such third-party software cannot be avoided, it should be installed by means of an intelligent risk management process that includes checking the software for malicious content (running anti-virus software, etc.).

1.4 Keep in mind that malicious programs are likely to use cameras as an entry point into an organization. To reduce supply chain risks, it is recommended to apply the same cyber defense and information security considerations as those implemented when introducing computer equipment inside or outside the organization.

2. Before installing the camera and during maintenance processes (if the use of components with Wi-Fi is unavoidable)

2.1 Enforce a strong authentication with the RADIUS or LDAP server and replace the Administrator's password and default passwords with a complex password (a long password that includes letters, numbers, and special characters) to reduce the risks of **dictionary and brute force attack**.

2.2 If it is not possible to acquire cameras without IoT components, it is recommended to disable Internet connectivity in the system settings (consider disabling the Wi-Fi in the OS level).

2.3 In cases in which an Internet connection is needed (for remote viewing or other considerations), ensure proper control and prevention of shut-off and automatic reporting to the Internet and to illegitimate addresses. Consider securing the communication medium with strong encryption (such as off-the-shelf encryption AES-256).

2.4 Be sure to perform software and firmware updates in accordance with the manufacturer's recommendations on secure and trusted channels in order to prevent manipulations and malware threats.[6]

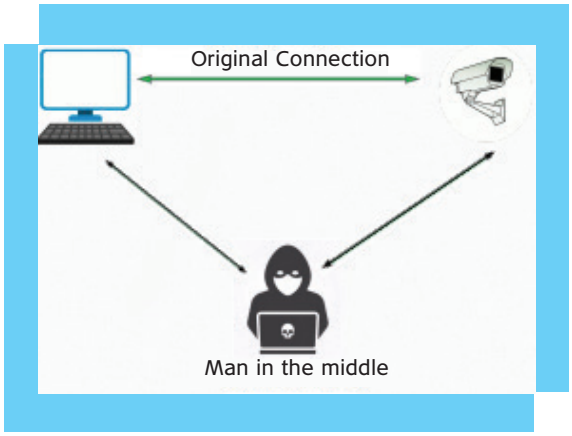
2.5 After each update, maintenance or upgrade, make sure that these definitions have not been modified and reset to their default values.

6 E.g., by having update files digitally signed by the manufacturer and sent through an encrypted medium

An example of disabling wireless capability at the operating system level

3. Segregating the camera in a standalone network or in a network by allocation of a dedicated Segment:

Isolating the camera in a **dedicated**, secure network in accordance with BP will significantly reduce accessibility and internal risks arising from the enterprise network, as well as the risks from communications with the camera or possible cyber events (DOS, DDOS attack, unauthorized viewing, network privacy, etc.).



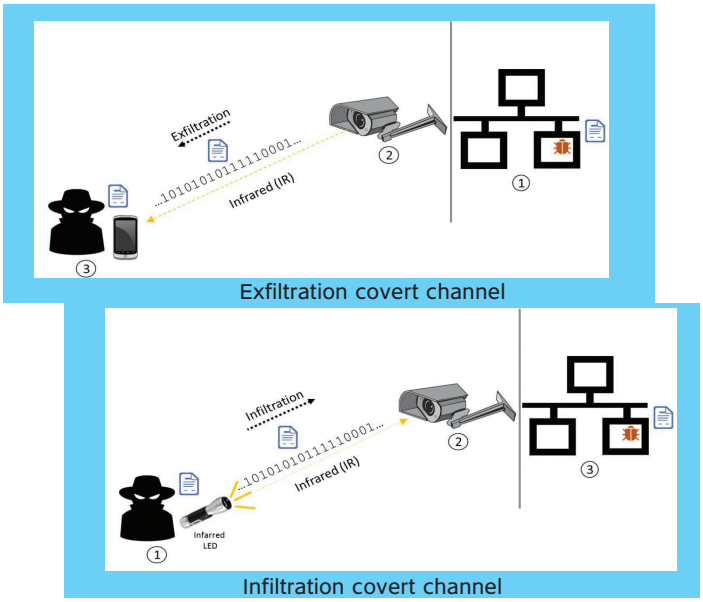
MITM scenario with an attacker in the middle (for unauthorized viewing and additional sophisticated attacks)

4. Using a segregated network

4.1 As a general rule, it is preferable to isolate the camera and security systems in a closed and secure network in accordance with BP in order to reduce threats from the Internet.

4.2 An appropriate solution must be found and the cyber risks arising from cameras segregated in closed networks should be reduced. **Options include access control, deception and camouflage, hardening of workstations, etc.** Various research projects have demonstrated the possibility of remotely accessing and attacking video surveillance cameras connected to closed networks for the purposes of exploitation and information retrieval or bridging to classified networks.[7]

4.3 It is recommended to consider **encrypting the communication media as an additional layer of security** (also on a closed network).



From the Study - aIR-Jumper: Covert Air-Gap Exfiltration/ Infiltration via Security Cameras & Infrared (IR) - Ben Gurion University

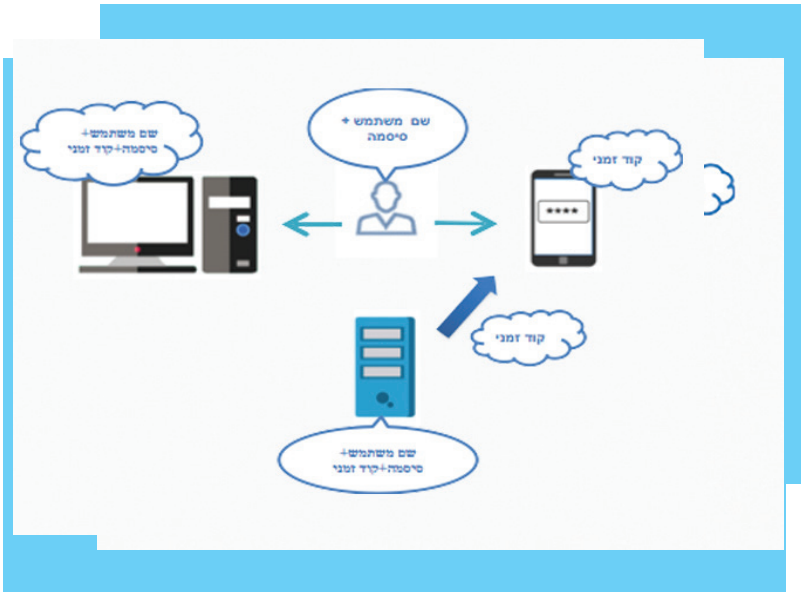
7 Mordechai Guri, Boris Zadov, and Yuval Elovici, "LED-it GO: Leaking (A Lot of) Data from Air-Gapped Computers via the (Small) Hard Drive LED". Detection of Intrusions and Malware and Vulnerability Assessment - 14th International Conference, DIMVA 2017: 161-184.

5. Using a dedicated VLAN (after the risk management process)

5.1 If the camera cannot be segregated in a closed network, a dedicated VLAN should be set up according to a common best practices principles for VLANs and secure architecture design. Firewall definitions should also be set and adapted rules implemented to monitor security incidents. Among other things, settings should be established to monitor unwanted communication with the cameras from outside the organization inwards and from inside the organization outwards.

5.2 It is recommended to review the technological settings to prevent DOS attacks (and thus prevent damage to the sequence of operations) and to implement appropriate **mitigation** controls by means of firewall settings, restricting the volume of traffic towards the cameras network, etc.

5.3 When faced with threats and documented attacks, it is recommended that all communications with the cameras be encrypted.



Remote two-step verification process

5.4 Computer permissions to view a camera from outside the organization require a stringent risk management procedure and reference to advanced authentication settings for user identification and the address of the designated component (For example: 2-step verification and computer address authorization by IP address approved by pre-defined white list), in order to prevent MITM threats and unauthorized use.

5.5 Computers and components licensed for viewing must be ruggedized in compliance with best terminal practices, or MDM for mobile components that are authorized for viewing (especially since these are remote components and not within the enterprise environment).

For additional network security recommendations, see the Organizational cyber security doctrine (available at www.gov.il/he/Departments/policies/cyber_security_methodology_for_organizations)[8].

For cloud connectivity, make sure to also implement protection controls for Cloud services (see: www.gov.il/BlobFolder/policy/cloud_services/he/Use%20of%20Cloud%20Services.pdf)[9].

6. Security settings for initial operation and general security settings

Leading video surveillance camera vendors offer to the system operators the ability to configure security settings during the installation stage, including:

6.1 Password lock mechanism for the camera. Some providers enable password lock settings in a mechanism that requires a strong password (Strong Password Enforcement)[10].

Sample screenshot from a manufacturer enforcing strong passwords upon installation

8 https://www.gov.il/he/Departments/policies/cyber_security_methodology_for_organizations

9 https://www.gov.il/BlobFolder/policy/cloud_services/he/Use%20of%20Cloud%20Services.pdf

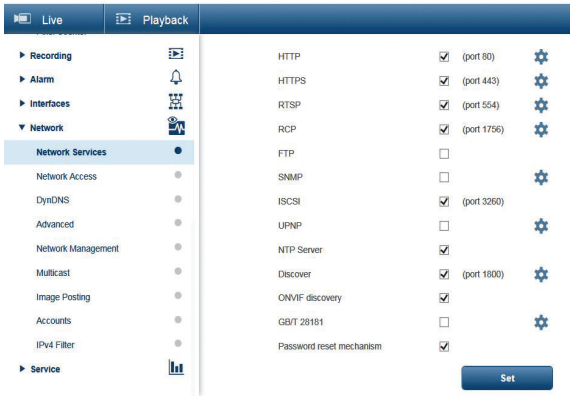
10 Best Practice Strong Password Enforcement - https://technet.microsoft.com/en-us/library/ff741764.aspx

6.2 Allocation and management of viewing permissions (3 levels: Level 1 - Permission to view live video; Level 2 - Permission to view live video, recordings and control; Level 3 - Administrator and/or technician authorization).

6.3 Local firewall settings to configure or block ports.

6.4 Blocking by default http communication.

6.5 Resources to prevent password reset.



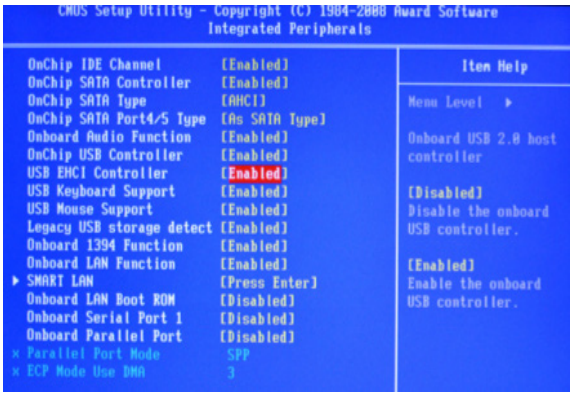
Example of the Network Service screen of one of the manufacturers

6.6 Use of the 802.1X protocol - This protocol configures access control between the client and the sever, so administrators can block unauthorized clients from accessing the LAN through available ports. (This also reduces MITM threats and unauthorized camera views)[11].

7. Physical security resources and prevention of access to the cameras and terminal equipment

7.1 As part of the process of reducing cyber risk and unauthorized handling of terminals (for theft, penetration of hostile code, etc.), **precautions must be taken to prevent access to video surveillance cameras** (elevating or isolating the cameras, etc.).

7.2 Removable media (all types of USB devices) are one of the most popular attack vectors.



Hence, a controlled reduction and neutralization of existing camera USB sockets should be performed.

7.3 Analytical tamper detection settings to detect camera shifting, liquid splashing, lens blur, focus change, loitering in the vicinity of the camera, nearby gatherings, etc.

11 Viewing permissions levels - Permission level 1 - Viewing live video permission, permission level 2 - Permission to view live video,
recordings and control, permission level 3 - Technician authorization

8 Reducing cyber risk in maintenance, support and camera handling processes

8.1 Make sure that cameras with controlled processes are handled only by authorized (trustworthy) personnel.

8.2 Update cameras in accordance with the manufacturer's recommendations and using secure and reliable processes (to prevent fraud, intermediation and MITM threats).

8.3 Change and harden Administrator passwords and default passwords to complex passwords in order to prevent unauthorized access and attacks based on the Default Password Index and password guessing.

8.4 The password policy should include prohibition of password sharing. Change passwords every six months (or according to the organization's policy) and during the turnover / departure process of any employee with access and authorization.

8.5 Ensure that the camera settings only allow firmware versions to be loaded from files signed by the manufacturer.

8.6 To reduce risks from bugs and hostile code, ensure that third-party software products or non-approved open-source software cannot be installed on the camera. Install source code segments after a code review process, using trusted elements and procedures, of the source code or of the segment to be installed (for example, compare the HASH files signed by the manufacturer during the software installation phase).

Bibliography

- Cyber Defence Methodology for an Organizations, Prime Minister's Office - Israel National Cyber Directorate, Version 1.0
- Best Practice Strong Password Enforcement - https://technet.microsoft.com/en-us/library/ff741764.aspx
- B. Krebs, "Hacked Cameras, DVRs Powered Today's Massive Internet Outage," October 2016.
- "Cameras & Infrared (IR)"
- "IoT Goes Nuclear: Creating a ZigBee Chain Reaction Eyal Ronen(B)". Colin O'Flynny, Adi Shamir and Achi-Or Weingarten, Weizmann Institute of Science, Rehovot, Israel
- Mordechai Guri, Boris Zadov, and Yuval Elovici, "LED-it-GO: Leaking (A Lot of) Data from Air-Gapped Computers via the (Small) Hard Drive LED". Detection of Intrusions and Malware and Vulnerability Assessment - 14th International Conference, DIMVA 2017: 161-184.
- Mordechai Guri, Dima Bykhovsky, and Yuval Elovicia, "IR-Jumper: Covert Air-Gap Exfiltration/Infiltration via Security"
- Mordechai Guri, Boris Zadov, Andrey Daidakulov, and Yuval Elovici, "xLED: Covert Data Exfiltration from Air-Gapped Networks via Router LEDs"

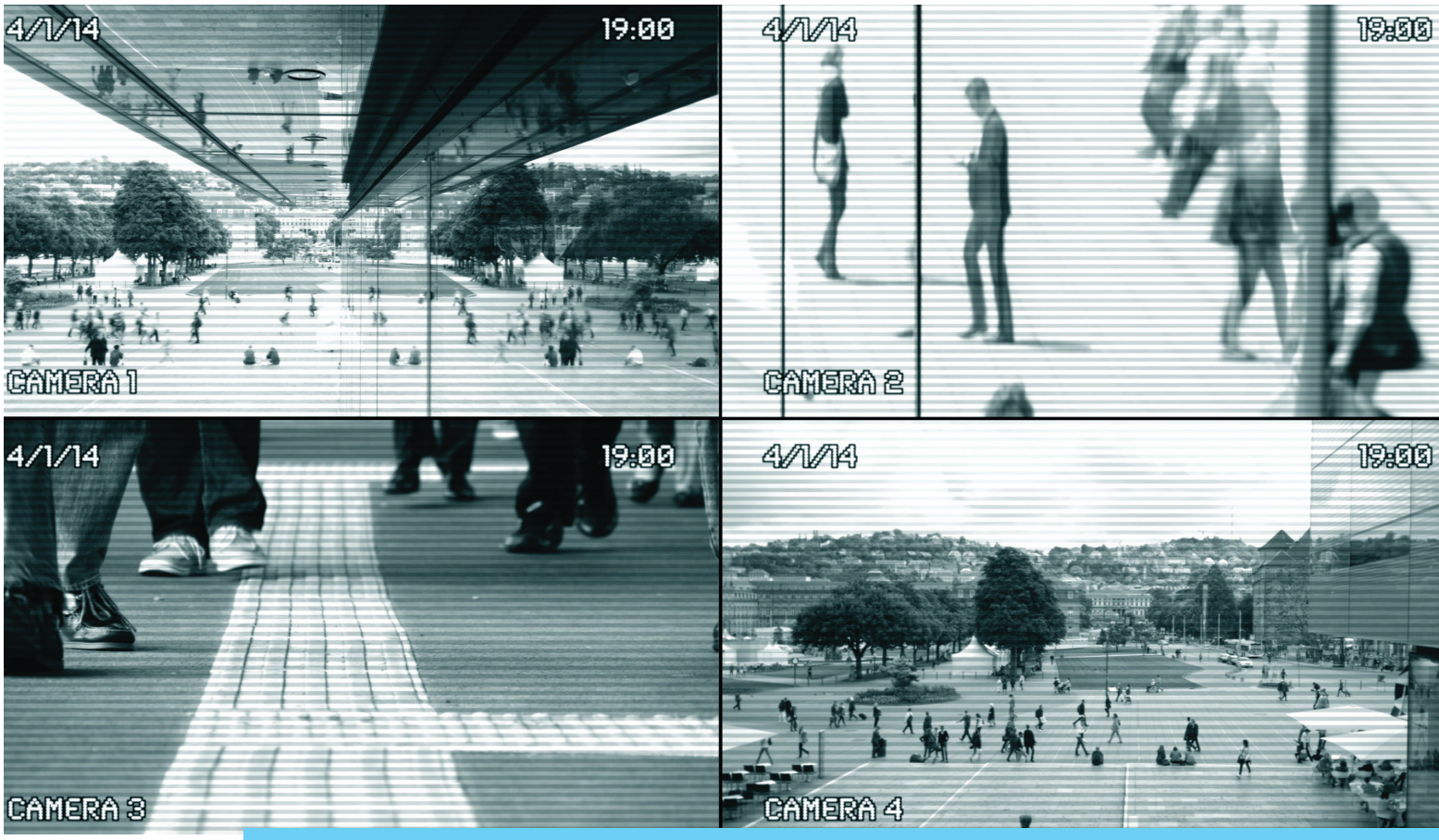
Appendices

Appendix A - Required resources and solutions for risk reduction (in various security layers)

	Reduction of unauthorized usage and viewing risks	Reduction of IoT risks	Reducing risk of traffic disruption or deletion of recordings	Reduction of DDOS risks of shutdown or denial of service	Penetration into the organization's systems via the camera network
Authentication	✔	✔	✔		
Allocation of a segregated network (depending on needs, organization and policy)	✔		✔	✔	✔
Allocation of a dedicated VLAN	✔		✔		
IoT security definitions	✔	✔	✔	✔	
Security resources for support and maintenance	✔	✔	✔		✔
Resources for camera segregation and access prevention	✔		✔		✔

Appendix B - Sample table for comparing requirements between manufacturers prior to acquisition

Mandatory requirement	Manufacturer A	Manufacturer B	Manufacturer C	Manufacturer D	Manufacturer E	Manufacturer F
3 security levels	✔	✔	✔	✔	✔	✔
Strong Password	✔	✔	✖	✖	✖	✔
Firmware signed Vendor	✖	✖	✖	✖	✔	✔
Disallow 3rd-party software	✖	✖	✖	✖	Partial	✔
SSL	✔	✔	✔	✔	✔	✔
Access prevention	✔	✔	✔	✔	✔	Partial
Encryption standards	✔	✖	✖	✖	✔	✔


4/1/14
19:00
CAMERA 1
4/1/14
19:00
CAMERA 2
4/1/14
19:00
CAMERA 3
4/1/14
19:00
CAMERA 4

Cyber Israel
Prime Minister's Office
National Cyber Directorate

119
tora@cyber.gov.il
www.cyber.gov.il
Find us