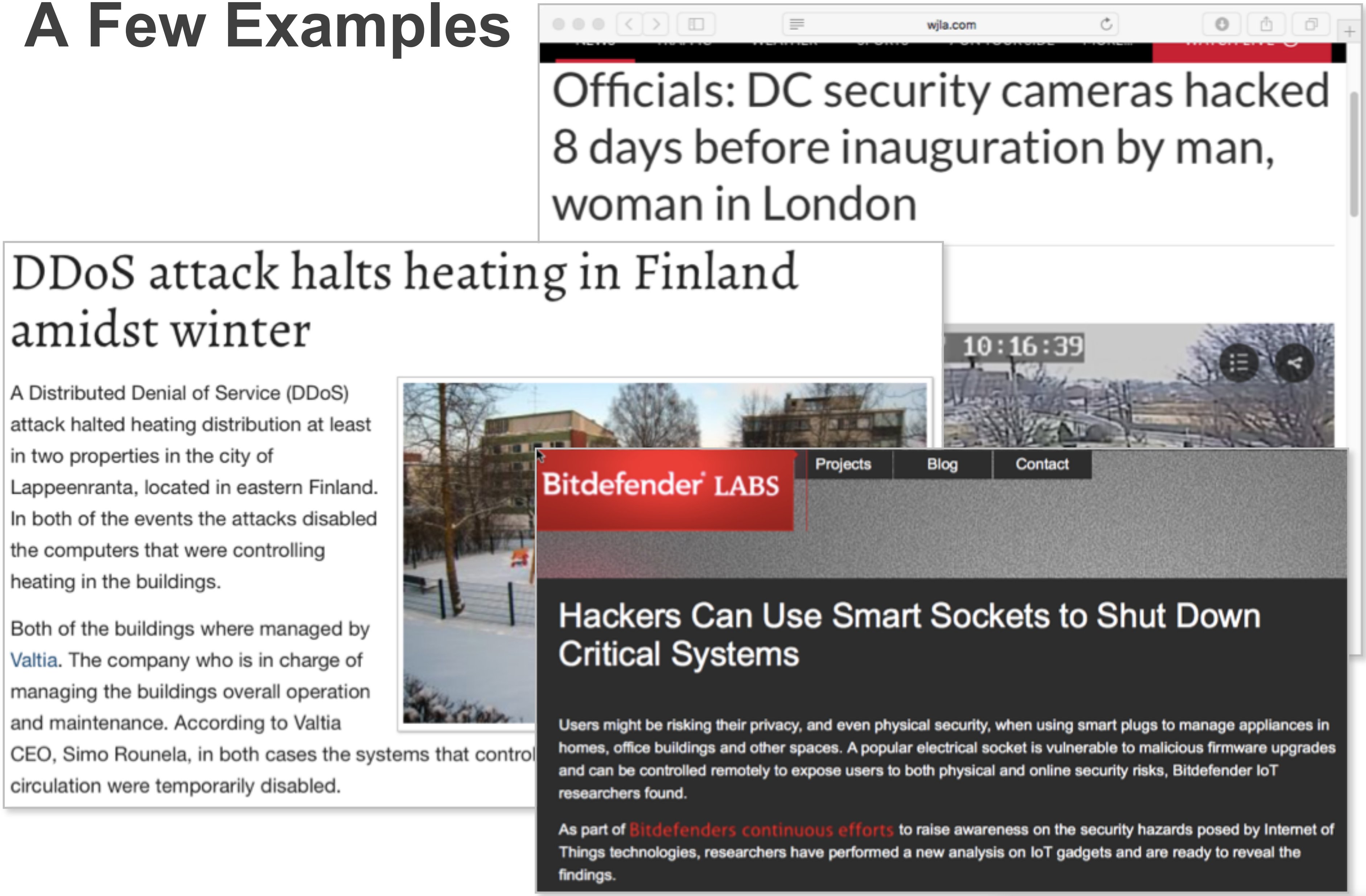
4º Congresso Brasileiro e Latino-Americano de IoT

Painel: Cybersecurity Group - an International joint effort.

Lucimara Desiderá, M.Sc.
lucimara@cert.br

cert.br nic.br cgi.br

Attacks to Smart Cities / IoT:
A Few Examples



Officials: DC security cameras hacked 8 days before inauguration by man, woman in London

DDoS attack halts heating in Finland amidst winter

A Distributed Denial of Service (DDoS) attack halted heating distribution at least in two properties in the city of Lappeenranta, located in eastern Finland. In both of the events the attacks disabled the computers that were controlling heating in the buildings.

Both of the buildings where managed by Valtia. The company who is in charge of managing the buildings overall operation and maintenance. According to Valtia CEO, Simo Rounela, in both cases the systems that contro circulation were temporarily disabled.

Bitdefender LABS

Hackers Can Use Smart Sockets to Shut Down Critical Systems

Users might be risking their privacy, and even physical security, when using smart plugs to manage appliances in homes, office buildings and other spaces. A popular electrical socket is vulnerable to malicious firmware upgrades and can be controlled remotely to expose users to both physical and online security risks, Bitdefender IoT researchers found.

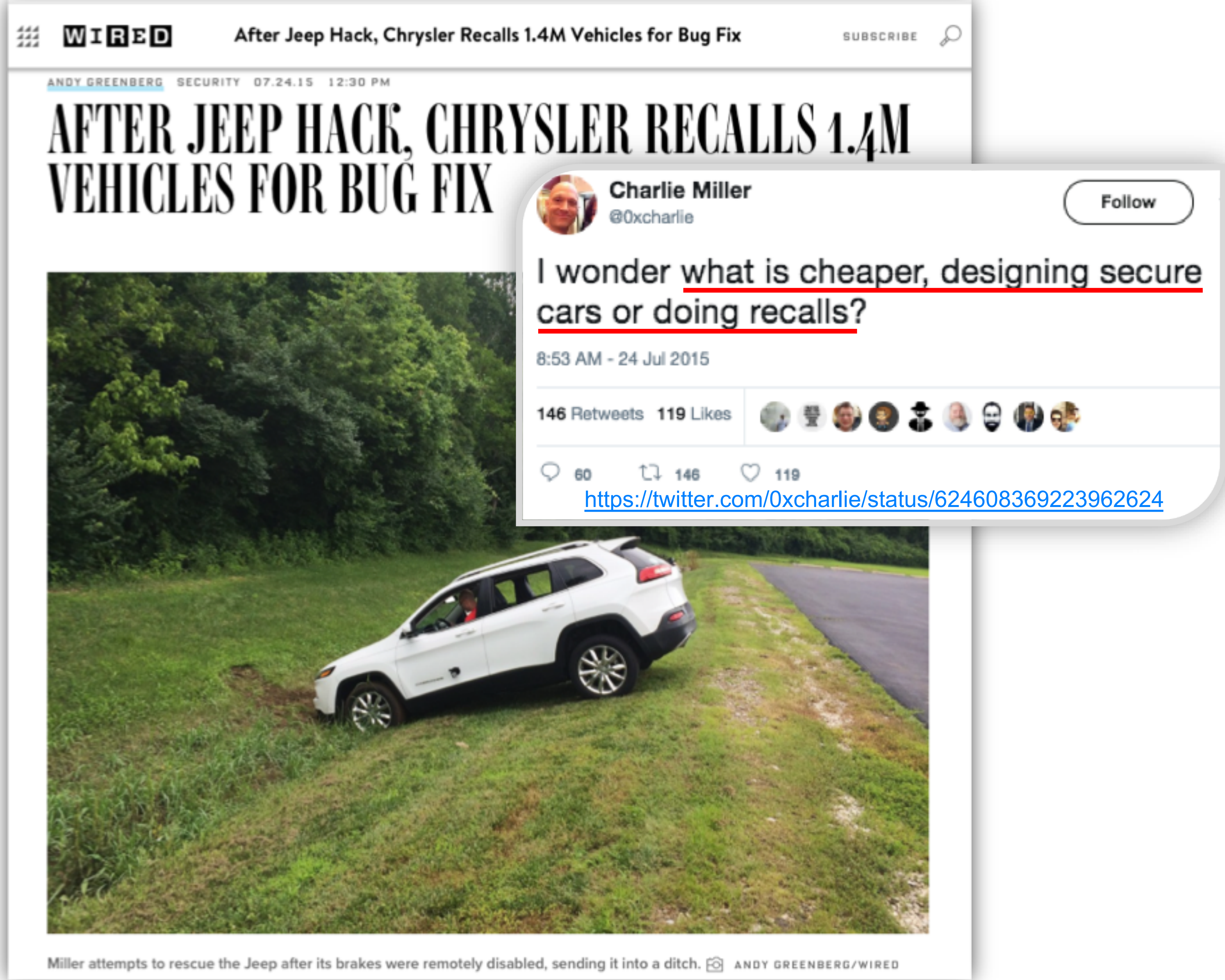
As part of Bitdefenders continuous efforts to raise awareness on the security hazards posed by Internet of Things technologies, researchers have performed a new analysis on IoT gadgets and are ready to reveal the findings.

There are many vulnerabilities in IoT:

- **Security is neglected**
  - even in security devices!
- **Few vendors have security updates lifecycle**
  - bug report mechanism
  - update distribution
- **Most of vendors repeat old mistakes:**
  - weak (or lack of) authentication
    - default common passwords/ hardcoded passwords / “*backdoors*”
  - Obsolete protocols without cryptography (ex: Telnet)
  - Unnecessary services enabled by default
- **Lack of a holistic view of security**
  - Device, mobile apps, network, cloud

What Should We Request from Developers/ Vendors / Manufacturers

- **Security must be *by design and by default***
  - not optional
  - consider security requirements since project initiation
  - use secure development best practices
  - secure factory defaults
- **Updates**
  - need to be possible and has to be secure (supply chain attacks)
- **Security should be included in the corporate risk management**
  - entire cities can stop in case of vulnerability
  - risk of damage to users
- **Plan for large scale updates**
- **Has to have a Product Security Incident Response Team (PSIRT) ➔ Maturity**



WIRED After Jeep Hack, Chrysler Recalls 1.4M Vehicles for Bug Fix SUBSCRIBE

ANDY GREENBERG SECURITY 07.24.15 12:30 PM

AFTER JEEP HACK, CHRYSLER RECALLS 1.4M VEHICLES FOR BUG FIX

Miller attempts to rescue the Jeep after its brakes were remotely disabled, sending it into a ditch. ANDY GREENBERG/WIRED

Charlie Miller
@0xcharlie
Follow

I wonder what is cheaper, designing secure cars or doing recalls?

8:53 AM - 24 Jul 2015

146 Retweets 119 Likes

60 146 119

https://twitter.com/0xcharlie/status/624608369223962624

https://www.wired.com/2015/07/jeep-hack-chrysler-recalls-1-4m-vehicles-bug-fix/

Minimum Security Requirements for Customer Premises Equipment (CPE) Acquisition

- Joint Publication of
  - M^{3}AAWG - Messaging, Malware and Mobile Anti-Abuse Working Group
  - LACNOG - Latin American and Caribbean Network Operators Group
  - Editor: Lucimara, LAC-AAWG Chair / CERT.br
- Currently available in:
  - English, Japanese and Korean
- New translations to be released soon:
  - Portuguese, Spanish, French and German

https://www.lacnog.net/docs/lac-bcop-1

https://www.m3aawg.org/CPESecurityBP

LACNOG- M³AAWG 공동 작성
CPE(가입자 댁내장치) 최소 보안 요구사항에 대한
Best Current Operational Practices
LAC-BCOP-1

2019 년 5 월

문서는 LACNOG 웹사이트에서 다운로드 가능합니다. www.lacnog.net/docs/lac-bcop-1

ityBP

P-Korean

WG[2]
ent
n and
WG
되었다.

.... 2
.... 2
.... 3
.... 4
.... 4
.... 5
.... 8
.... 9
.... 9
.... 9
.... 10
.... 12

M³AAWG
Working Group
reet, Suite 302
w.m3aawg.org

LACNOG-M³AAWG 共同作業による
顧客側通信機器 (CPE) が備えるべき
最低限のセキュリティ要件についての
Best Current Operational Practices
LAC-BCO

May 2019

この文書の原文は LACNOG の Web サイト www.la

この文書の原文は M³AAWG の Web サイト www.m

この文書は LACNOG[1] (Latin American and Caribbean N
(Messaging, Malware and Mobile Anti-Abuse Working Gro
Current Operational Practices (BCOP)である。LACNOG
AAWG[3] (Latin American and Caribbean Anti-Abuse Work
した草案をもとに M³AAWG 会員と Senior Technical A
調作業によって作成された。

[1] Latin American and Caribbean Network Operators Group (LACNOG
[2] Messaging, Malware and Mobile Anti-Abuse Working Group (M³AAV
[3] Latin American and Caribbean Anti-Abuse Working Group (LAC-AA
[4] LACNOG BCOP Working Group, https://www.lacnog.net/wg-bcop

LACNOG
Latin American and Caribbean Network Operators Group
Department of Montevideo, Oriental Republic of Uruguay
www.lacnog.net

LACNOG-M³AAWG Joint Best Current Operational Practices on Minimum Security Requirements for Customer Premises Equipment (CPE) Acquisition LAC-BCOP-1

May 2019

This document is available on the LACNOG website at www.lacnog.net/docs/lac-bcop-1

This document is available on the M³AAWG website at www.m3aawg.org/CPESecurityBP

This is a joint Best Current Operational Practices (BCOP) document developed by LACNOG[1] (Latin American and Caribbean Network Operators Group) and M³AAWG[2] (Messaging, Malware and Mobile Anti-Abuse Working Group). It is the product of LACNOG's original drafts by its working groups LAC-AAWG[3] (Latin American and Caribbean Anti-Abuse Working Group) and BCOP Working Group[4], in cooperation with M³AAWG members, Senior Technical Advisors and the M³AAWG Technical Committee.

Table of Contents

[1] The Latin American and Caribbean Network Operators Group (LACNOG), https://www.lacnog.net/
[2] Messaging, Malware and Mobile Anti-Abuse Working Group (M3AAWG), https://www.m3aawg.org/
[3] Latin American and Caribbean Anti-Abuse Working Group (LAC-AAWG), https://www.lacnog.net/lac-aawg/
[4] LACNOG BCOP Working Group, https://www.lacnog.net/wg-bcops/

LACNOG
Latin American and Caribbean Network Operators Group
Department of Montevideo, Oriental Republic of Uruguay
www.lacnog.net

M³AAWG
Messaging, Malware and Mobile Anti-Abuse Working Group
781 Beach Street, Suite 302
San Francisco, California 94109 U.S.A. – www.m3aawg.org

What is inside?

A reference checklist for hardware decisions

→ Let’s ask vendors for better products while improving our networks!

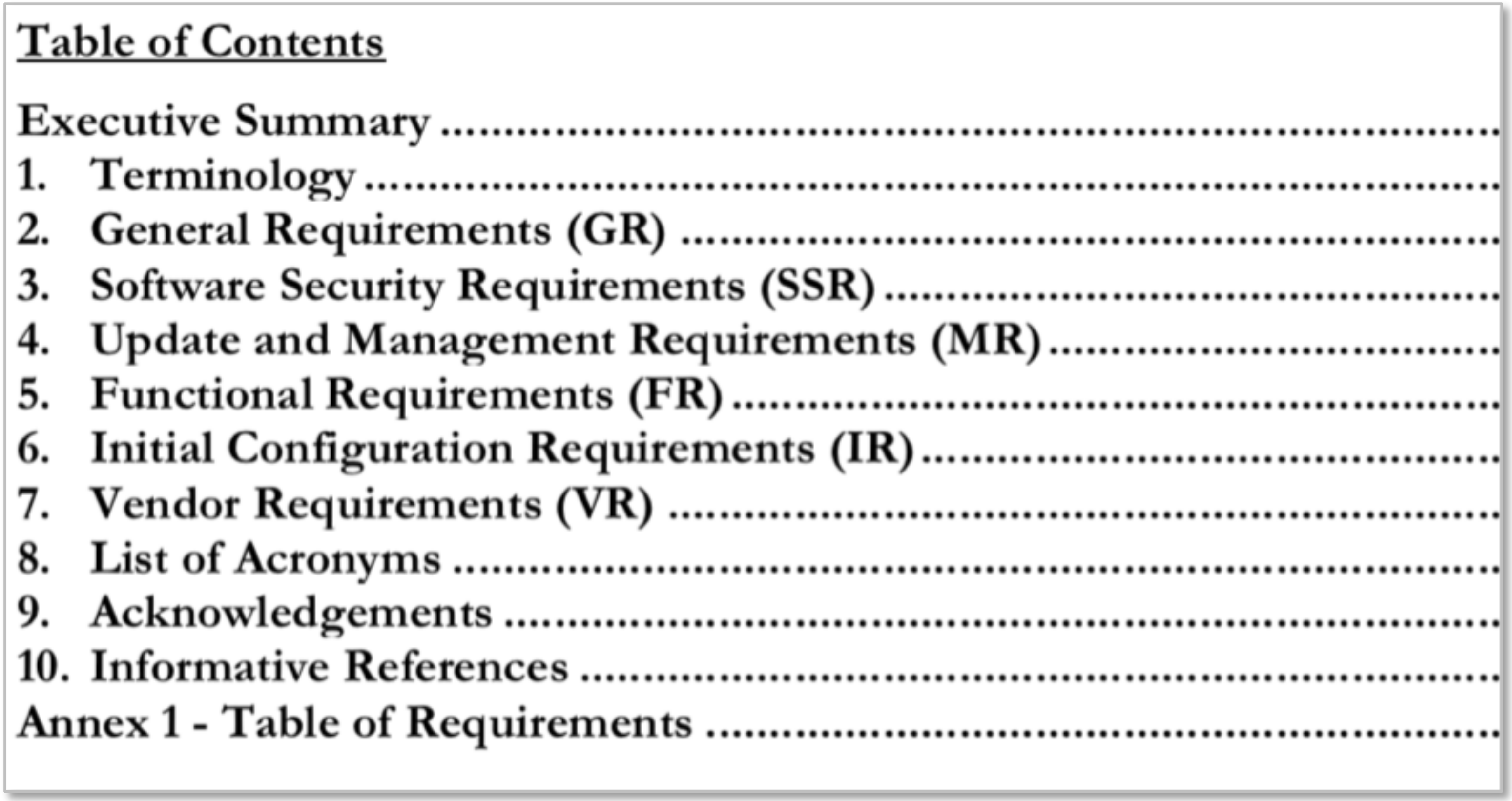
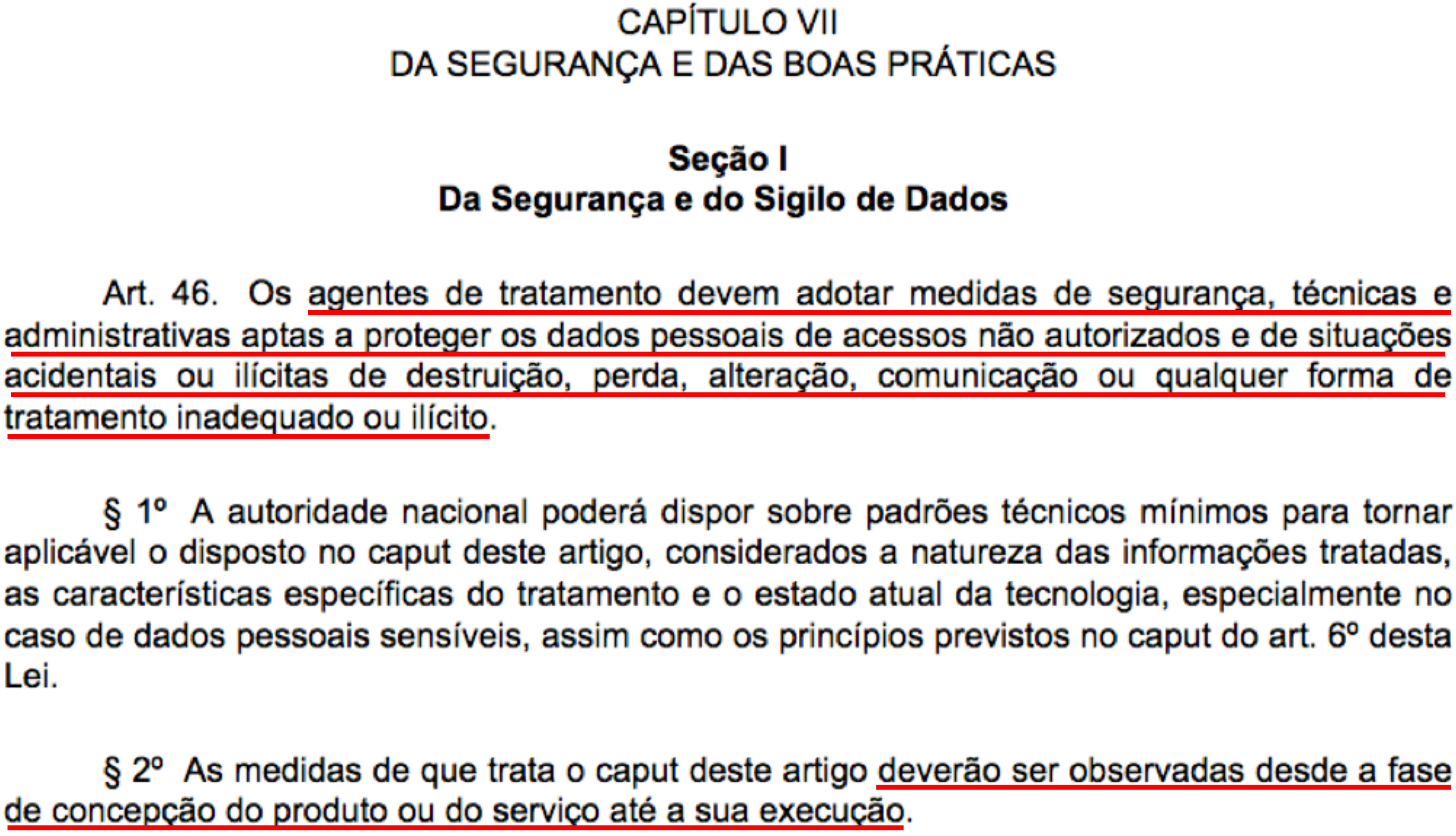


Table of Contents



CAPÍTULO VII
DA SEGURANÇA E DAS BOAS PRÁTICAS

Seção I
Da Segurança e do Sigilo de Dados

Art. 46. Os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito.

§ 1º A autoridade nacional poderá dispor sobre padrões técnicos mínimos para tornar aplicável o disposto no caput deste artigo, considerados a natureza das informações tratadas, as características específicas do tratamento e o estado atual da tecnologia, especialmente no caso de dados pessoais sensíveis, assim como os princípios previstos no caput do art. 6º desta Lei.

§ 2º As medidas de que trata o caput deste artigo deverão ser observadas desde a fase de concepção do produto ou do serviço até a sua execução.

http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm