ČESKÁ TECHNICKÁ NORMA

ICS 33.020; 35.030; 35.240.95

Leden 2021

CYBER – Kybernetická bezpečnost pro internet věcí spotřebitele: základní požadavky

ČSN
ETSI EN 303 645
V2.1.1
87 0030

CYBER – Cyber Security for Consumer Internet of Things: Baseline Requirements

Tato norma přejímá anglickou verzi evropské normy ETSI EN 303 645 V2.1.1:2020. Má stejný status jako oficiální verze.

This standard implements the English version of the European Standard ETSI EN 303 645 V2.1.1:2020. It has the same status as the official version.

Anotace obsahu

Tento dokument stanovuje vysokoúrovňová opatření pro bezpečnost a ochranu osobních údajů pro zařízení IoT spotřebitele, která jsou připojena k síťové infrastruktuře (jako je například internet nebo domácí síť), a jejich interakce s přidruženými službami. Tyto přidružené služby leží mimo rozsah platnosti. Neúplný seznam příkladů zařízení IoT spotřebitele zahrnuje:

- připojené dětské hračky a chůvičky;
- připojené detektory kouře, dveřní zámky a okenní senzory;
- brány, základnové stanice a uzly IoT, k nimž se připojuje více zařízení;
- inteligentní kamery, televizní přijímače a reproduktory;
- nositelné zdravotnické sledovací prostředky;
- připojené domácí automatizační a poplachové systémy, zejména jejich brány a uzly;
- připojené spotřebiče, jako jsou například pračky a chladničky; a
- inteligentní domácí asistenti.

Kromě toho tento dokument řeší bezpečnostní úvahy specifické pro omezená zařízení (například okenní kontaktní senzory, povodňové senzory a elektrické spínače).

Tento dokument poskytuje prostřednictvím příkladů a vysvětlujícího textu návod pro organizace, zapojené do vývoje a výroby IoT spotřebitele, na způsob implementace těchto opatření.

Zařízení, která nejsou zařízeními IoT spotřebitele, například ta, která jsou především určena k použití ve výrobě, zdravotní péči nebo jiných průmyslových aplikacích, nejsou v rozsahu platnosti

tohoto dokumentu.

Národní předmluva

Informace o citovaných dokumentech

ETSI TR 103 305-3 nezavedena

ETSI TR 103 309 nezavedena

Speciální publikace NIST 800-63B nezavedena (dostupná na https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63b.pdf)

ISO/IEC 29147 zavedena v ČSN EN ISO/IEC 29147 (36 9713) Informační technologie – Bezpečnostní techniky – Odhalování zranitelností (dostupná na https://www.iso.org/standard/45170.html)

OASIS: Společný rámec vykazování zranitelnosti (CVRF) CSAF nezaveden (dostupný na http://docs.oasis-open/CSAF/CSAF-cvrf/v1.2/csaf-cvrf-v1.2.html)

ETSI TR 103 331 nezavedena

ENISA: Základní bezpečnostní doporučení pro IoT v kontextu kritických informačních infrastruktur, listopad 2017, ISBN: 978-92-9204-236-2, doi:10.2824/03228 nezavedeno (dostupné na https://op.europa.eu/en/publication-detail/-/publication/c37f8196-d96f-11e7-a506-01aa75ed71a1/language-en/format-PDF/source-117211901)

Ministerstvo UK pro digitalizaci, kulturu, média a sport: Bezpečné designem: Zpráva o zdokonalování kybernetické bezpečnosti internetu věcí spotřebitele, březen 2018 nezavedena (dostupná na https://www.gov.uk/government/collections/secure-by-design)

Fond pro bezpečnost IoT: Rámec shody o bezpečnosti IoT, vydání 2, prosinec 2018 nezaveden (dostupný na https://www.iotsecurityfoundation.org/wp-content/uploads/2018/12/IoTSF-IoT-SecurityCompliance-Framework-Release-2.0-December-2018.pdf)

GSMA: Bezpečnostní pokyny a hodnocení IoT GSMA nezavedeny (dostupné na https://www.gsma.com/iot/iot-security/iot-security-guidelines/)

ETSI TR 103 533 nezavedena

Sdělení Komise: „Modrá příručka“ k provádění pravidel EU pro výrobky 2016 (text s významem pro EHP), 2016/C 272/01 nezavedeno (dostupné v Úředním věstníku Evropské unie, https://eur-lex.europa.eu/legalcontent/EN/ALL/?uri=OJ:C:2016:272:TOC.)

Copper Horse: Mapování bezpečnosti a soukromí v internetu věcí nezavedeno (dostupné na https://iotsecuritymapping.uk/)

ENISA: Základní bezpečnostní doporučení pro IoT – interaktivní nástroj nezavedeno (dostupné na https://www.enisa.europa.eu/topics/iot-and-smart-infrastructures/iot/baseline-securityrecommendations-for-iot-interactive-tool)

Fond pro bezpečnost IoT: Chápání současného využití zveřejňování zranitelnosti ve výrobních společnostech internetu věcí spotřebitele nezavedeno (dostupné na https://www.iotsecurityfoundation.org/wp-content/uploads/2018/11/VulnerabilityDisclosure-Design-v4.pdf)

F-Secure: Hrozby IoT: Exploze „chytrých zařízení“ zaplňující domácnosti vede ke zvýšeným rizikům nezavedeno (dostupné na https://blog.f-secure.com/iot-threats/)

W3C: Web věcí na W3C nezavedeno (dostupné na https://www.w3.org/WoT/)

ETSI TS 103 701 nezavedena (zpracovává se)

DIN SPEC 27072 nezavedena

GSMA: Program koordinovaného zveřejňování zranitelnosti nezaveden (dostupný na https://www.gsma.com/security/gsma-coordinated-vulnerability-disclosure-programme/)

Fond pro bezpečnost IoT: Zveřejňování zranitelnosti – pokyny pro nejlepší postupy nezavedeno (dostupné na https://www.iotsecurityfoundation.org/wp-content/uploads/2017/12/VulnerabilityDisclosure_WG4_2017.pdf)

OWASP: Internet věcí (IoT), nejdůležitějších 10:2018 nezavedeno (dostupné na https://www.owasp.org/index.php/OWASP_Internet_of_Things_Project#tab=IoT_Top_10.)

IEEE 802.15.4™-2015 nezavedena (dostupná na https://standards.ieee.org/content/ieee-standards/en/standard/802_15_4-2015.html.)

ETSI TS 102 221 nezavedena

GSMA: Technická specifikace SGP.22 v2.2.1 nezavedena

ISO/IEC 27005:2018 zavedena v ČSN ISO/IEC 27005:2019 (36 9790) Informační technologie – Bezpečnostní techniky – Řízení rizik bezpečnosti informací (dostupná na https://www.iso.org/standard/75281.html)

Microsoft® Corporation: Model hrozeb STRIDE nezaveden (dostupný na https://msdn.microsoft.com/en-us/library/ee823878(v=cs.20).aspx.)

ETSI TR 121 905 nezavedena

POZNÁMKA Pokud jsou v originálu normy citovány nezaváděné dokumenty ETR, TBR, ES, EG, TS, TR a GSM, jsou dostupné v zákaznickém centru ČAS.

Citované předpisy

Nařízení (EU) 2016/679 Evropského parlamentu a Rady ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (95/46/EC) (obecné nařízení o ochraně osobních údajů).

Vysvětlivky k textu této normy

V případě nedatovaných odkazů na evropské/mezinárodní normy jsou ČSN uvedené v článku „Informace o citovaných dokumentech“ nejnovějšími vydáními, platnými v době schválení této normy. Při používání této normy je třeba vždy použít taková vydání ČSN, která přejímají nejnovější vydání nedatovaných evropských/mezinárodních norem (včetně všech změn).

Upozornění na národní přílohu

Do této normy byla doplněna národní příloha NA, která obsahuje překlad kapitoly 3 této evropské normy.

Vypracování normy

Zpracovatel: MAREŠKA Praha, IČO 86983555, Ing. Antonín Mareška

Technická normalizační komise: TNK 96 Telekomunikace

Pracovník České agentury pro standardizaci: Ing. Jan Křivka

Česká agentura pro standardizaci je státní příspěvková organizace zřízená Úřadem pro technickou normalizaci, metrologii a státní zkušebnictví na základě ustanovení § 5 odst. 2 zákona č. 22/1997 Sb., o technických požadavcích na výrobky a o změně a doplnění některých zákonů, ve znění pozdějších předpisů.