



У Д И Т Ё Л И

XVIII национална научна конференция с международно участие



**ОБЩЕСТВОТО НА ЗНАНИЕТО
И ХУМАНИЗМЪТ НА XXI ВЕК**

1 ноември 2020 г.

ПРЕГЛЕД НА РЕГУЛАТОРНАТА БАЗА В ОБЛАСТТА НА КИБЕРСИГУРНОСТТА НА ICS

Светлана Сярова

Университет по Библиотекознание и Информационни Технологии

Предизвикателствата в областта на киберсигурността на ICS са от решаващо значение за правителствата, непрекъснатостта на бизнеса и неприкосновеността на личния живот. За целта на прегледа разделям регулаторните мерки в три основни области:

- законодателни инициативи;
- международни и отраслови стандарти;
- рамки за конструиране на Кибер защитата на ICS.

Прегледът включва кратък анализ на причините за нарастване на регулаторните мерки за повишаване на нивото на Кибер защита на ICS. Обхваща законодателните и стандартизационни инициативи от страните с развити дигитални инфраструктури в различни отрасли на икономиката. Характеризира се с интегриран подход към интердисциплинарния характер на проблема.

Целта на прегледа е да проуча съдържанието на документите от тази проблемна област и да ги систематизирам. За постигането на тази цел се решават следните задачи:

- 1) Проучване на съществуващите стандарти;
- 2) Въвеждане на признаци и подреждане на стандартите по класове и групи;
- 3) Извеждане на недостатъците и предимствата им.

Много държави са приели закони или стратегии за киберсигурност, базирани на световно признати документи, пригаждайки ги съгласно своята инфраструктура и специфика.

Държава	Име на документа
Австралия	Cyber Security Strategy, 2009 г.
България	Закон за киберсигурност, 2018 г.
Великобритания	The UK Cyber Security Strategy, 2011 г.
Германия	Cyber Security Strategy for Germany, 2011 г.
Европейски Съюз	Cybersecurity Act 2017 г.
Индия	Discussion draft on National Cyber Security Policy, 2011г.
Канада	Canada's Cyber Security Strategy, 2010 г.
Китай	Cyberspace Administration of China-CAC, 2014 г.
Нидерландия	The National Cyber Security Strategy, 2011 г.
Нова Зеландия	New Zealand Cyber Security Strategy, 2011 г.
Русия	Доктрина информационной безопасности Российской Федерации, 2016 г.
САЩ	National Cyber Strategy the United State of America, 2018
Северна Корея	Korea Internet & Security Agency KISA, 2009 г.
Япония	National center of Incident readiness and Strategy for Cybersecurity-NISC 2015 г.

Действащи регулации в различни държави, както и кратко описание:

Акт	Резюме	Потребители
NIST (National Institute of Standards and Technology)	Рамка, предоставяща персонализирано ръководство за управление и намаляване на риска, свързан с киберсигурността	Може да бъде приложена от всяка организация, която иска да намали общия си риск
CIS Controls (Center for Internet Security Controls)	Защита на активите и данните на организацията от известни вектори за кибер атаки	Компании, които се стремят да засилят сигурността в интернет на нещата (IoT)
ISO 27000 Family	Фамилия от стандарти, даваща препоръки за сигурност при поддържане на системите за управление на ИС чрез прилагане на контроли за сигурност	Всички фирми могат да се възползват от тези стандарти за оценка на своите практики за киберсигурност
ISO 31000 Family	Набор от регулации, уреждащ принципите на прилагане и управление на риска	Всички фирми могат да се възползват от тези регулации за оценка на своите практики за киберсигурност
HIPAA (Health Insurance Portability and Accountability Act)	Този акт е законопроект. Защищава правото на медицинско обслужване при смяна на работа или освобождаване от работа. Също така цели да опрости процеса на здравеопазване чрез преминаване към електронни данни и да защити поверителността на отделните пациенти	Всяка организация, която обработва данни
PCI-DSS (Payment Card Industry Data Security Standard)	Набор от 12 наредби, предназначени да намалят измамите и да защитят информацията за кредитните карти на клиента	Компании, които обработват информация за кредитни карти
GDPR (General Data Protection Act)	Регламентира защитата и поверителността на личните данни на гражданите на ЕС	Всяка компания, която обработва данни на граждани на ЕС
SOX (Sarbanes-Oxley Act)	Този акт изисква компаниите да поддържат финансови записи до седем години	Публични дружества в САЩ, мениджмънт и публични счетоводни фирми
COBIT (Control Objectives for Information and Related Technologies)	Тази рамка е разработена, за да помогне на организациите в управлението на информацията и технологиите чрез свързване на бизнес и ИТ цели	Организации, които отговарят за бизнес процесите, свързани с технологиите и контрола на качеството на информацията
FISMA (Federal Information Security Modernization Act of 2014)	Този акт признава сигурността на информацията като въпрос на националната сигурност и задължава всички федерални агенции да разработят метод за защита на своите ИС	Всички федерални агенции попадат в обхвата на този законопроект
COPPA (Children's Online Privacy Protection Rule)	Онлайн събиране на лична информация за деца под 13 години	Всяко лице или организация под юрисдикцията на САЩ
NERC CIP Standards (NERC Critical Infrastructure Protection)	Подобряване на сигурността на енергийната система на Северна Америка	Всички собственици и оператори в електроенергийната система

Основните стандарти и придружаващите ги документи, свързани с Директивата NIS за сигурността на ICS:

Системи за управление на ИС за предоставяне на насоки и най-добри практики за управление на ИТ

ISO/IEC 27000	Системи за управление на информационната сигурност Преглед и речник
ISO/IEC 27001	Системи за управление на информационната сигурност Изисквания
ISO/IEC 27002	Кодекс на практиката за контрол на информационната сигурност
ISO/IEC 27005	Управление на риска от информационна сигурност
ISO/IEC 27007	Системи за управление на информационната сигурност- Насоки за одитори
ISO/IEC 27008	Насоки за одитори за контрол на ISMS
ISO/IEC 27009	Приложение на ISO/IEC 27001, специфично за сектора– Изисквания
ISO/IEC 27019	Насоки за управление на информационната сигурност, базирани на ISO/IEC 27002 за системи за управление на процеси, специфични за енергийната индустрия

Техники за оценка и методи за гарантиране на сигурност:

ISO/IEC 15408	Общи критерии
ISO/IEC 15446	Ръководство за изготвяне на защитни профили и цели за сигурност
ISO/IEC 17825	Характеристика на атаките на страничните канали
ISO/IEC 18045	Метод за оценка на общи критерии
ISO/IEC 18367	Криптографски алгоритми и защитни механизми за тестване на съответствието
ISO/IEC 19608	Ръководство за разработване на функционални изисквания за сигурност и поверителност въз основа на ISO/IEC 15408
ISO/IEC 19790	Изисквания за сигурност на криптографските модули
ISO/IEC 19896	Изисквания за компетентност за тестери и оценители на информационна сигурност
ISO/IEC 19989	Оценка на сигурността на откриване на атака при представяне на биометрични показатели
ISO/IEC 27032	Насоки за киберсигурност
ISO/IEC 27034	Защита на приложенията
ISO/IEC 27035	Управление на инциденти в сигурността на информацията
ISO/IEC 27036	Информационна сигурност за връзки с доставчици

Сравнение на част от стандартите по основни критерии.

	ISO 27002	API 1164	IEEE 1711.2	AGA 12	NERC	NIST 800-53	IEC 62351	ANSI/ISA-62443	ISA-TR99.00.02	NIST PCSRF	IEC 62210	IEC 62443
ПОЛИТИКА ЗА СИГУРНОСТ SECURITY POLICY												
Политика за информационна сигурност	√	√	√	√	√	√	√	√	√	√	√	√
УЯЗВИМОСТ И ОЦЕНКА НА РИСКА VILNERABILITY AND RISK ASSESSMENT												
Уязвимост и оценка на риска	√			√	√		√	√	√	√		
ОРГАНИЗАЦИОННА СИГУРНОСТ												
Инфраструктура за информационна сигурност	√		√	√	√	√			√	√	√	
Сигурност на достъпа на трети страни	√	√	√	√		√			√	√	√	
Аутсорсинг	√			√		√					√	
КЛАСИФИКАЦИЯ И УПРАВЛЕНИЕ НА АКТИВИ												
Отчетност на активи	√					√	√	√	√	√	√	
Информационна класификация	√	√					√	√			√	
ЛИЧНА СИГУРНОСТ												
Сигурност при определяне на работата и ресурси	√	√	√	√	√	√	√	√	√	√		
Обучение на потребителите	√	√	√	√	√	√	√	√	√	√		
Отговор на инцидент със сигурност и неизправности	√	√		√	√	√	√		√	√		

СИСТЕМНО РАЗВИТИЕ И ПОДДРЪЖКА												
Изисквания за сигурност на системите	√	√			√	√	√	√	√		√	√
Сигурност в приложни системи	√					√	√	√	√		√	√
Криптографски контроли	√	√	√	√	√			√	√		√	√
SCADA -изисквания за компонентите на криптографската система				√				√			√	√
Управление на ключовете				√	√		√	√			√	√
Сигурност на системните файлове	√			√			√					√
Сигурност в процесите на развитие и поддръжка	√					√	√	√	√			
Управление на кръпките за сигурност	√	√			√		√	√	√			
УПРАВЛЕНИЕ НА НЕПРЕКЪСНАТОСТТА НА БИЗНЕСА												
Аспекти на управлението на непрекъснатостта на бизнеса					√		√			√		
Изисквания за съответствие на системата SCADA	√	√			√	√	√		√	√		
СЪОТВЕТСТВИЕ												
Процес на мониторинг на съответствието						√	√		√			
Проверка на съоръженията						√	√		√			
Спазване на законовите изисквания			√				√	√		√		
Съображения относно системния одит	√						√	√	√	√	√	√
ПЛАН ЗА ТЕСВАНЕ CRYPTOGRAPHICSYSTEMTESTPLAN												
План за тестване на криптографската система			√	√								√

Европейски стандарти

Европейската програма за защита на критичната инфраструктура (EPCIP—European Programme for Critical Infrastructure Protection) определя общата рамка за дейности, насочени към подобряване на защитата на критичната инфраструктура в Европа. Основен стълб на EPCIP става Директивата за европейската критична инфраструктура от 2008 г. През 2013 г. е приета Директива 2013/40/ЕС относно атаките срещу информационните системи. През 2016 е приета Директива 2016/1148/ЕС за мрежова и информационна сигурност. Директива 1148 излиза почти едновременно с Регламент (ЕС) 2016/679 за защита на данните (GDPR), който има за цел да хармонизира законодателството, защитавайки данните.

С Регламент (ЕС) 1025/2012 **CEN**, **CENELEC** и **ETSI** са признати за европейски организации по стандартизация -ЕСО:

CEN (French: Comité Européen de Normalisation) или Европейският комитет по стандартизация отговаря за дейностите по стандартизация във всички области, с изключение на електротехнологията и телекомуникациите;

CENELEC (European Committee for Electrotechnical Standardization) или Европейският комитет по електротехническа стандартизация отговаря за дейностите по стандартизация в електротехническата област;

ETSI (European Telecommunications Standards Institute) или Европейският институт за далекосъобщителни стандарти отговаря за дейностите по стандартизация в областта на ИКТ и телекомуникациите.

През 2017 г. CEN и CENELEC създават нов съвместен технически комитет, TC 13 по „Киберсигурност и защита на данните“, който възнамерява да разработва стандарти и насоки в подкрепа на политиките на ЕС.

Техническите органи на ETSI подготвят документи, свързани със стандартизацията, които могат да бъдат използвани в подкрепа на спазването на NISD (European Network and Information Security Directive).

Резултати

Съществуват голям брой стандарти и препоръки, които са от значение за сигурността. Това проучване започна с изчерпателно търсене на документи, изготвени от органи по стандартизация и правителствени агенции. В това търсене бяха използвани следните критерии, за да се определи дали даден стандарт (или насока) ще бъде включен в нашата таблица:

- Стандартът е наличен на английски език;
- Стандартът се публикува от орган по стандартизация или правителствена агенция;
- Стандартът е съсредоточен върху сигурността на ICS (а не ИТ или информационната сигурност като цяло);
- Стандартът/насоката трябва да се фокусира върху ICS системи като цяло.

Осем стандарта и насоки или групи отговарят на тези изисквания:

Documents	Publisher
Good Practice Guide, Process Control and SCADA Security	Centre for the Protection of National Infrastructure (CPNI)
Cyber Security Procurement Language for Control Systems	Department of Homeland Security (DHS)
21 steps to Improve Cyber Security of SCADA Networks	U.S. Department of Energy (DOE)
CIP-002-1 - CIP-014-2	North American Electric Reliability Corporation (NERC)
Guide to Industrial Control Systems (ICS) Security	National Institute of Standards and Technology (NIST)
System Protection Profile - ICS	National Institute of Standards and Technology (NIST)
ANSI/ISA–99.00.01–2007	The International Society of Automation (ISA)
Cyber security for Critical Infrastructure Protection	U.S. Government Accountability Office (U.S. GAO)

Заклучения

Нуждите на институциите, както е описано в много източници, се отнасят до разработването на ефективни подходи за оценка на сложните инфраструктури. Ефективността на всяко предложено решение се фокусира върху необходимото време и данни, нужни за един модел. Способността да се обхване всеки вид риск на нивото, на което резултатът от анализа да допринесе за процеса на вземане на решения, е ключов фактор. Във всички случаи понятието за устойчивост (resilience) на инфраструктурата изглежда липсващ елемент. За по-пълно въвеждане на концепцията за устойчивост следва да се извърши цялостна оценка на инфраструктурата, засилена координация между заинтересованите страни и своевременно реагиране на всички взаимосвързани критични инфраструктури. Трябва да има хармоничен подход, който да включва превенция, устойчивост и мерки за възстановяване, насочен към непрекъснатата работа на инфраструктурата.

Изводите ни са както следва:

- Навлизането на новите регулаторни изисквания се отразява в начина на организиране и експлоатация на ICS;
- Предизвиква процеси на трансформация и изисква автоматизирано управление на защитата (SOC).

БЛАГОДАРЯ!