پیوست

شورای اجرایی (عالی) فناوری اطلاعات کشور

کمیسیون توسعه دولت الکترونیکی

چارچوب معماری سازمانی ایران

معماری مرجع امنیت

استانداردهای امنیتی حوزه شبکه و اینترنت اشیا

نسخه ۱,۰ – اردیبهشت ماه ۱۳۹۶

پیشگفتار

نیازمندی‌های امنیت اطلاعات در داخل سازمان دستخوش دو تغییر عمده در چندین دهه اخیر شده است. پیش از گسترش به کارگیری تجهیزات پردازش داده، نیاز اساسی امنیت اطلاعات در سازمان فراهم نمودن وسایل مدیریتی و فیزیکی می‌باشد. با ظهور رایانه‌ها، نیاز به ابزارهای خودکار برای حفاظت فایل‌ها و دیگر اطلاعات ذخیره شده بر روی رایانه بدیهی است. حفاظت، پشتیبانی و نگهداری از داده‌های رایانه‌ای، اطلاعات مهم، برنامه‌های حساس، نرم‌افزارهای مورد نیاز و یا هر آنچه که در حافظه جانبی رایانه مورد توجه بوده و با اهمیت می‌باشد، امنیت رایانه‌ای نامیده می‌شود.

تغییر عمده دوم که متاثر از امنیت اطلاعات است معرفی سیستم‌های توزیع شده و به کارگیری شبکه و تسهیلات ارتباطی برای حمل داده میان کاربر ترمینال و رایانه یا بین دو رایانه می‌باشد. اقدامات امنیتی شبکه نیاز به حفاظت داده حین انتقال آن‌ها دارند. در حقیقت واژه امنیت شبکه به مدت زیادی گمراه کننده بود زیرا تقریبا تمام کسب و کارها، دولت و سازمان‌های دانشگاهی با به کارگیری تجهیزات پردازش داده خود و مجموعه‌ای از شبکه‌های بهم پیوسته از جمله اینترنت، به یکدیگر متصل بودند. با توجه به انتشار انواع بدافزارها از جمله ویروس‌ها و کرم‌ها در بستر اینترنت و شبکه‌های رایانه‌ای، هیچگونه خط مرزی میان دو واژه امنیت رایانه و شبکه نمی‌توان قایل شد.

تفکر امنیت در شبکه برای دستیابی به سه مولفه مهم محرمانگی، صحت و در دسترس پذیری است. این سه مولفه اصول اساسی امنیت اطلاعات در شبکه و یا بیرون آن را تشکیل می دهند به گونه‌ای که تمامی تمهیدات و سازوکارهای لازمی که برای امنیت شبکه اتخاذ می‌شود و یا تجهیزاتی که ساخته می‌شوند، همگی ناشی از نیاز به اعمال این سه پارامتر در محیط های نگهداری و تبادل اطلاعات است.

لازم به ذکر است که فناوری رو به رشد اینترنت اشیاء نیز از بستر شبکه و اینترنت استفاده می‌کند. این فناوری تاثیرات گسترده‌ای را بر روی سازمان‌ها، استراتژی کسب و کار، مدیریت ریسک و مجموعه‌ای وسیع از سایر حوزه‌های فنی نظیر معماری و طراحی شبکه به دنبال دارد.

اینترنت اشیاء، به معنی امکان برقراری ارتباط تمام اشیاء با یکدیگر و با انسان‌ها، به همراه شناسایی و کشف آن‌ها تحت یک شبکه یکپارچه است. طبیعی است که ایجاد چنین شبکه‌ای، مخاطرات فراوانی را به همراه دارد. شبکه جهانی اینترنت که از همگانی شدن آن سال‌ها می‌گذرد، هنوز دارای ضعف‌های امنیتی بسیاری در خود است که موجب به خطر افتادن اموال و حتی جان انسان‌ها نیز شده است. در چنین شرایطی، برقراری امنیت در یک شبکه جهانی از اشیاء که هر کدام با ویژگی‌ها و محدودیت‌های خود به ارتباط با یکدیگر و با انسان‌ها می‌پردازند، طبیعتا از پیچیدگی بسیار بالاتری برخوردار خواهد بود. شرایط جدید محیط و ویژگی‌های مختلف دستگاه‌ها، سبب می‌شود تا امنیت اینترنت اشیاء به طور ویژه مورد توجه قرار بگیرد و معماری‌های متعددی برای آن ارایه شود.

همچنین به دلیل وجود بحث مالکیت اشیاء و همین‌طور حفظ حریم خصوصی افراد، توجه به نکات امنیتی مرتبط با شناسایی و کشف، دسترس‌پذیری، کنترل دسترسی، حریم خصوصی و اعتماد نیز در اینترنت اشیاء از اهمیت بیشتری برخوردار خواهد بود.

لیست کلی استانداردهای حوزه شبکه و اینترنت اشیاء در ادامه مشخص شده است.

نام استاندارد	شماره استاندارد
A Role-Based Model for Federal Information Technology/Cybersecurity Training, Rev 1, (2014) یک مدل مبتنی بر نقش برای آموزش امنیت سایبری/ فناوری اطلاعات فدرال	SP 800-16
Security Considerations in the System Development Life Cycle, Rev. 2, (2008) ملاحظات امنیتی در چرخه حیات توسعه سیستم	SP 800-64
Risk Management Guide for Information Technology Systems, (2002) راهنمای مدیریت ریسک برای سیستم‌های فناوری اطلاعات	SP 800-30
Guidelines on Firewalls and Firewall Policy, (2009) راهنمایی‌هایی در مورد دیواره آتش و سیاست‌های آن	SP 800-41
Guidelines on Securing Public Web Servers, rev 2, (2007) راهنمایی در مورد امنیت وب سرورهای عمومی	SP 800-44
Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security, Rev.2, (2016) راهنمایی برای امنیت دورکاری سازمان‌ها، دسترسی از راه دور و استفاده از دستگاه‌های شخصی (BYOD)	SP 800-46
Guide to Securing Legacy IEEE 802.11 Wireless Networks, Rev 1, (2008) راهنمایی برای تامین امنیت شبکه‌های بی‌سیمIEEE 802.11	SP 800-48
Security and Privacy Controls for Federal Information Systems and Organizations, Rev 4, (2013) کنترل‌های امنیتی و حریم خصوصی برای سازمان‌ها و سیستم‌های اطلاعاتی فدرال	SP 800-53
Assessing Security and Privacy Controls in Federal Information Systems and Organizations, (2014) ارزیابی امنیتی و کنترل‌های حریم خصوصی در سازمان‌ها و سیستم‌های اطلاعات فدرال	SP 800-53A
Computer Security Incident Handling Guide, rev 1, (2012) راهنمای رسیدگی به حوادث امنیتی کامپیوتری	SP 800-61
Secure Domain Name System (DNS) Deployment Guide, Rev 2, (2013) راهنمای استقرار امن سیستم نام دامنه	SP 800-81
Guide to Computer Security Log Management, (2006)	SP 800-92

راهنمایی برای مدیریت وقایع امنیتی کامپیوتر	
Guide to Intrusion Detection and Prevention Systems (IDPS), Rev 1, (2012) راهنمایی برای سیستم‌های تشخیص و پیشگیری از نفوذ	SP 800-94
Guide to Secure Web Services, (2007) راهنمایی برای امنیت سرویس‌های وب	SP 800-95
Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11i, (2007) ایجاد شبکه‌های امنیتی مستحکم بی‌سیم: راهنمایی برای IEEE 802.11i	SP 800-97
Guide to SSL VPNs, (2008) راهنمایی برای شبکه خصوصی مجازی مبتنی بر لایه سوکت امن	SP 800-113
Guidelines for the Secure Deployment of IPv6, (2010) راهنمایی برای توسعه امن IPv6	SP 800-119
Recommendation for EAP Methods Used in Wireless Network Access Authentication, (2009) توصیه‌هایی برای روش‌های پروتکل احراز هویت توسعه‌پذیر به‌کار رفته در احرازهویت دسترسی به شبکه بی‌سیم	SP 800-120
Guide to General Server Security, (2008) راهنمایی برای امنیت سرویس‌دهنده عمومی	SP 800-123
Secure Virtual Network Configuration for Virtual Machine (VM) Protection, (2016) پیکربندی امن شبکه مجازی جهت حفاظت ماشین مجازی	SP 800-125B
Guide to Securing WiMAX Wireless Communications, (2010) راهنمایی برای امن‌سازی ارتباطات بی‌سیم WiMAX	SP 800-127
Guide for Security-Focused Configuration Management of Information Systems, (2011) راهنمایی برای مدیریت پیکربندی متمرکز بر امنیت سیستم‌های اطلاعاتی	SP 800-128
Guide to Cyber Threat Information Sharing, (2016) راهنمایی برای به اشتراک‌گذاری اطلاعات تهدید سایبری	SP 800-150
Guidelines for Securing Wireless Local Area Networks (WLANs), (2012) راهنمایی برای امن‌سازی شبکه‌های محلی بی‌سیم	SP 800-153

Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations, Rev 1, (2016) حفاظت از اطلاعات غیرمحرمانه کنترل شده در سازمان‌ها و سیستم‌های غیر فدرال	SP 800-171
Guideline for Using Cryptographic Standards in the Federal Government: Directives, Mandates and Policies, (2016) راهنمایی برای استفاده از استانداردهای رمزنگاری در دولت فدرال: دستورالعمل‌ها، تعهدات و سیاست‌ها	SP 800-175A
Guideline for Using Cryptographic Standards in the Federal Government: Cryptographic Mechanisms, (2016) راهنمایی برای استفاده از استانداردهای رمزنگاری در دولت فدرال: مکانیسم‌های رمزنگاری	SP 800-175B
Guide for Cybersecurity Event Recovery, (2016) راهنمایی برای بازیابی رویداد امنیت سایبری	SP 800-184
Standards for Security Categorization of Federal Information and Information Systems, (2004) استانداردهایی برای طبقه‌بندی سیستم‌های اطلاعاتی و اطلاعات فدرال	FIPS 199
Minimum Security Requirements for Federal Information and Information Systems, (2006) حداقل الزامات امنیتی برای سیستم‌های اطلاعاتی و اطلاعات فدرال	FIPS 200
Security Requirements for Cryptographic Modules, (2001) نیازمندی‌های امنیتی برای ماژول‌های رمزنگاری	FIPS 140-2
ISO/IEC 27033: Information technology — Security techniques — Network security, (2010) استاندارد امنیت شبکه	ISO/IEC 27033
ISO/IEC 27035:2016 Information technology — Security techniques — Information security incident management, (2016) مدیریت حوادث امنیتی	ISO/IEC 27035
ISO/IEC 27039:2015 — Information technology — Security techniques — Selection, deployment and operation of intrusion detection and prevention systems (IDPS), (2015) انتخاب، استقرار و عملیات سیستم‌های تشخیص و جلوگیری از نفوذ (IDPS)	ISO/IEC 27039
MIME-Based Secure Peer-to-Peer Business Data Interchange Using HTTP, Applicability Statement 2 (AS2), (2005) مبادله امن داده‌های کسب و کار نظیر به نظیر مبتنی‌بر MIME با استفاده از HTTP، بیانیه کاربردی	RFC 4130
DNS Security Introduction and Requirements, (2005) نیازمندی‌ها و معرفی امنیت DNS	RFC 4033

Resource Records for the DNS Security Extensions, (2005) رکوردهای منبع برای توسعه امنیت DNS	RFC 4034
Protocol Modifications for the DNS Security Extensions, (2005) اصلاحات پروتکل برای توسعه امنیت DNS	RFC 4035
Storing Certificates in the Domain Name System (DNS), (2006) ذخیره‌سازی گواهینامه‌ها در سیستم نام دامنه (DNS)	RFC 4398
Using DNS to Securely Publish Secure Shell (SSH) Key Fingerprints, (2006) استفاده از DNS برای انتشار اثر انگشت‌های کلید SSH به صورت امن	RFC 4255
The DNS-Based Authentication of Named Entities (DANE) Protocol: Updates and Operational Guidance, (2015) پروتکل احراز هویت مبتنی بر DNS موجودیت‌های نام‌گذاری شده (DANE): راهنمایی عملی و بروزرسانی‌ها	RFC 7671
Source Address Validation Improvement (SAVI) Solution for DHCP, (2015) راه حل بهبود اعتبارسنجی آدرس مبداء[1] برای DHCP	RFC 7513
DHCPv6-Shield: Protecting against Rogue DHCPv6 Servers, (2015) پوشش محافظ DHCPv6؛ حفاظت در برابر سرویس‌دهنده‌های متقلب DHCPv6	RFC 7610
Transport Layer Security (TLS) Transport Model for the Simple Network Management Protocol (SNMP), (2011) مدل انتقال TLS برای پروتکل SNMP	RFC 6353
BGP Operations and Security, 2015 امنیت و اقدامات BGP	RFC 7454
Transport Layer Security (TLS) Session Resumption without Server-Side State, (2008) نشست مجدد TLS بدون در نظرگیری وضعیت سمت سرویس‌دهنده	RFC 5077
Transport Layer Security (TLS) Application-Layer Protocol Negotiation Extension, (2014) ضمیمه مذاکره پروتکل TLS مبتنی بر لایه کاربرد	RFC 7301
Using the NETCONF Protocol over Secure Shell (SSH), (2011) استفاده از پروتکل NETCONF بر روی پوسته امن (SSH)	RFC 6242

[1] Source Address Validation Improvement

DIGITAL CELLULAR TELECOMMUNICATIONS SYSTEM (PHASE 2+) (GSM)/ UNIVERSAL MOBILE TELECOMMUNICATIONS SYSTEM (UMTS)/ LTE/ GENERIC AUTHENTICATION ARCHITECTURE (GAA)/ GENERIC BOOTSTRAPPING ARCHITECTURE (GBA), (2016) سیستم‌های مخابرات دیجیتال تلفن همراه (GSM)- سیستم جهانی ارتباطات راه دور موبایل- فناوری تکامل بلند مدت (LTE)- سرویس‌های همه پخشی/چندپخشی چندرسانه‌ای	ETSI TS 133 220
Analysis of Security Solutions for the oneM2M System, (2014) تجزیه و تحلیل راه‌حل‌های امنیتی برای سیستم oneM2M	ETSI TS 118 508
Digital Enhanced Cordless Telecommunications (DECT)/Common Interface (CI)/ Part 7: Security features, (2015) ارتباطات بی‌سیم پیشرفته دیجیتالی/رابط مشترک/ بخش۷: ویژگی‌های امنیتی	ETSI EN 300 175-7
IEEE Standard for Information Technology: Hardcopy Device and System Security, (2010) استاندارد IEEE برای فناوری اطلاعات: دستگاه چاپی و امنیت سیستم	IEEE 2600-2008
The Transport Layer Security (TLS) Protocol, (2008) پروتکل امنیتی لایه انتقال(TLS)	RFC 5246
Authentication and Authorization for Constrained Environments (ACE), (2016) احرازهویت و مجوزدهی برای محیط‌های محدود شده	
Information security management systems, (2016) سیستم مدیریت امنیت اطلاعات	ISO/IEC 27000-series
Security Services (SAML) TC, (2012) سرویس‌های امنیتی (زبان نشانه گذاری تاکید امنیتی)	
eXtensible Access Control Markup Language (XACML) TC, (2013) زبان نشانه‌گذاری قابل گسترش کنترل دسترسی	
Security solutions, (2016) راحل‌های امنیتی	ETSI TS 118 103
provides a privacy framework, (2011) ارایه چارچوب حفظ حریم خصوصی	ISO/IEC 29100

XML Key Management Specification, (2005)	
مشخصات مدیریت کلید XML	
IEEE Cyber Security for the Smart Grid, (2013)	
امنیت سایبر برای شبکه هوشمند	

- **NIST SP 800-16: A Role-Based Model for Federal Information Technology/ Cybersecurity Training, Rev 1, (2014)**

این سند یک چارچوب مفهومی جدید را برای آموزش امنیت فناوری اطلاعات ارایه می‌دهد. این چارچوب شامل نیازمندی‌های آموزش امنیت فناوری اطلاعات برای محیط محاسبات توزیع شده است. رویکرد آموزش در این سند براساس اصول زیر طراحی شده است:

- تمرکز بر روی توابع کار، یا نقش‌ها و مسئولیت‌ها
- ترسیم تفاوت میان آگاهی و آموزش
- ارایه یک چارچوب یکپارچه برای شناسایی نیازمندی‌های آموزشی و اطمینان از اموزش‌های مناسب
- ارایه یک ابزار توسعه
- ارایه یک ساختار برای ارزیابی اثربخشی یادگیری

- **NIST SP 800-30: Risk Management Guide for Information Technology Systems, (2002)**

مدیریت ریسک، یکی از جنبه‌های کلیدی مدیریت امنیت است که نقش مهمی در حفاظت از دارایی‌های اطلاعاتی دارد. سند SP 800-30 با مرور کلی از مدیریت ریسک آغاز شده و مواردی که منجر به موفقیت برنامه مدیریت ریسک می‌شود را پوشش می‌دهد. این راهنما همچنین نشان می‌دهد که چگونه مدیریت ریسک، قادر به یکپارچه‌سازی چرخه حیات توسعه سیستم می‌شود. این سند همچنین مواردی مانند طبقه‌بندی کنترل، تحلیل سود و زیان، ارزیابی ریسک باقی‌مانده و گزینه‌های کاهش آن و نیز مراحلی که باید پس از اتمام روند ریسک درنظر گرفته شوند را شامل می‌شود.

- **NIST SP 800-41: Guidelines on Firewalls and Firewall Policy, (2009)**

هدف این سند کمک به سازمان‌ها در درک قابلیت‌های فناوری‌های دیواره آتش و سیاست‌های دیواره آتش می‌باشد. در واقع قابلیت‌های امنیتی و مزایا و معایب دیواره آتش را بررسی کرده و همچنین راهنمایی‌های کاربردی را در توسعه سیاست‌های دیواره‌آتش و انتخاب، پیکربندی، تست، استقرار و مدیریت دیواره آتش فراهم می‌کند.

برای بهبود اثربخشی و امنیت دیواره‌آتش، سازمان‌ها باید توصیه‌های زیر را پیاده‌سازی کنند:

- ایجاد سیاست دیواره آتش که مشخص می‌کند دیواره آتش چگونه باید ترافیک شبکه‌های ورودی و خروجی خود را مدیریت کند.
- شناسایی تمام نیازمندی‌هایی که بایستی در زمان تعیین دیواره اتش برای پیاده‌سازی در نظر گرفته شود.
- مدیریت معماری دیواره آتش، سیاست‌ها، نرم‌افزار، و دیگر اجزا در سراسر حیات راه‌حل‌های دیواره آتش

- **NIST SP 800-44: Guidelines on Securing Public Web Servers, rev 2, (2007)**

هدف این سند ارایه توصیه‌هایی در مورد اقدامات امنیتی برای طراحی و پیاده‌سازی سرورهای وب در دسترس عموم، از جمله مسایل مربوط به زیرساخت‌های شبکه می‌باشد. این سند توسط سازمان‌ها برای افزایش امنیت سرورهای وب موجود و آینده استفاده شده تا تعداد و تکرار حوادث امنیتی مربوط به سرورهای وب را کاهش دهد. همچنین اصول عمومی ارایه شده را به تمام سیستم عامل‌ها اعمال می‌کند.

این سند جنبه‌های مربوط به تامین امنیت وب سرور را پوشش نمی‌دهد. از جمله:

- ملاحظات امنیتی مربوط به سرویس‌گیرنده وب
- امن کردن انواع متفاوت سرورهای شبکه
- دیواره‌های آتش و مسیریاب‌های مورد استفاده برای حفاظت سرویس‌دهنده پست الکترونیک

- **NIST SP 800-46: Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security, Rev.2 (2016)**

هدف از این سند، کمک به سازمان‌ها در کاهش ریسک‌های مرتبط با فناوری‌های سازمانی مورداستفاده در دورکاری، مانند دسترسی از راه دور سرویس‌دهنده‌ها، دورکاری دستگاه‌های سرویس‌گیرنده و ارتباطات دسترسی از راه دور است. این سند بر اهمیت تامین امنیت اطلاعات حساس ذخیره شده در دستگاه‌های دورکاری و انتقال از طریق دسترسی از راه دور در سراسر شبکه خارجی تاکید کرده و همچنین توصیه‌هایی برای ایجاد سیاست‌های مرتبط با دورکاری و برای انتخاب، پیاده‌سازی و حفظ کنترل‌های امنیتی لازم برای دسترسی از راه دور به سرویس‌دهنده و سرویس‌گیرنده را ارایه می‌دهد.

- **NIST SP 800-48: Guide to Securing Legacy IEEE 802.11 Wireless Networks, Rev 1, (2008)**

هدف این سند فراهم نمودن راهنمایی برای سازمان‌ها جهت امنیت شبکه‌های بی‌سیم خود براساس استاندارد IEEE 802.11 است که نمی‌توانند از استاندارد IEEE 802.11i استفاده کنند. جزئیات درباره امن نمودن قابلیت WLANها در IEEE 802.11i در استاندارد NIST 800-97 وجود دارند.

توصیه‌نامه‌ها برای امنیت در به‌کارگیری WLAN خارجی، از جمله نقاط دسترسی عمومی بی‌سیم خارج از دامنه این سند می‌باشد.

- **NIST SP 800-53: Security and Privacy Controls for Federal Information Systems and Organizations, Rev 4, (2013)**

این نشریه یک کاتالوگ از کنترل‌های امنیتی و حفظ حریم خصوصی برای سیستم‌های اطلاعات فدرال و سازمان‌ها فراهم می‌کند. همچنین فرایندی برای انتخاب کنترل‌های مناسب برای محافظت از عملیات سازمانی (رسالت، توابع، نمود و شهرت)، دارایی‌های سازمانی، افراد، سازمان‌های دیگر و ملت از مجموعه‌ای

متنوع از تهدیدات از جمله حملات خصمانه سایبری، بلایای طبیعی، شکست‌های ساختاری و خطاهای انسانی ارایه می‌دهد. لازم به ذکر است که نسخه پنج این سند در دست تهیه است.

- **NIST SP 800-53A: Assessing Security and Privacy Controls in Federal Information Systems and Organizations, (2014)**

هدف از این نشریه ارایه راهنمایی‌هایی برای ایجاد طرح‌های ارزیابی امنیتی موثر و مجموعه‌ای جامع از روش‌ها برای اثربخشی کنترل‌های امنیتی به کار گرفته شده در سیستم‌های اطلاعاتی می‌باشد. این دستورالعمل‌ها برای کنترل‌های امنیتی تعریف شده در استاندارد SP 800-53 استفاده می‌شود.

مخاطبان این نشریه:

- افراد مسئول توسعه و یکپارچه‌سازی سیستم اطلاعات
- افرادی که مسئول ارزیابی و نظارت امنیت اطلاعات هستند.
- افراد مسئول نظارت، مدیریت امنیت
- افرادی که مسئول پیاده‌سازی امنیت اطلاعات هستند.

- **NIST SP 800-61: Computer Security Incident Handling Guide, rev 1, (2012)**

تهدیدهایی که در گذشته عمر کوتاهی داشته و به آسانی پیدا می‌شدند، امروزه جای خود را به تهدیدات مداوم پیشرفته[۲] (APTها) داده‌اند و این امر، ضرورت استفاده از رویه‌های رسیدگی به حوادث را نشان می‌دهد. استاندارد SP 800-61، سازمان‌ها را در توسعه رویه‌های رسیدگی به حوادث و کنترل تهدیدات امنیتی یاری می‌کند. این استاندارد برای تیم‌های پاسخگویی به حوادث[۳] مفید است.

---

[2] Advanced Persistent Threats

[3] Incident Response Team

- **NIST SP 800-64: Security Considerations in the System Development Life Cycle, Rev. 2, (2008)**

در نسخه‌دوم این استاندارد به طور مستقیم به امنیت نرم‌افزار پرداخته شده است چرا که این سند، راهنمایی‌هایی را برای پیاده‌سازی امنیت درون چرخه حیات توسعه سیستم یا نرم‌افزار ارایه می‌دهد و به طیف گسترده‌ای از مخاطبان سیستم‌های اطلاعاتی و کارشناسان امنیت اطلاعات اعم از صاحبان سیستم، صاحبان اطلاعات، توسعه‌دهندگان و مدیران برنامه خدمت می‌کند.

- **NIST SP 800-81: Secure Domain Name System (DNS) Deployment Guide, Rev 2, (2013)**

هدف این نشریه کمک به سازمان‌ها در درک توسعه امن سرویس‌های DNS در یک سازمان می‌باشد و یک راهنمای عملی برای امن نمودن هر وجه از DNS را در داخل سازمان بر پایه تحلیلی از یک محیط عملیاتی و تهدیدات مرتبط ارایه می‌دهد. در حال حاضر، DNS هدف اکثر حملات نیست اما باتوجه به امن‌تر شدن میزبان‌ها و وابستگی برنامه‌های کاربردی به زیر ساخت DNS به منظور انجام عملیات شبکه، زیرساخت DNS به هدف وسوسه برانگیزی تبدیل خواهد شد. از این رو استفاده از DNSSEC وسیله‌ای برای امنیت شبکه می‌با شد. در این راهنما تو سعه DNNSEC تنها در زیر ساخت DNS مورد هدف قرار گرفته و به میزبان‌های شخصی توجهی ندارد. این استاندارد برای استفاده مدیران توسعه DNS و همچنین کارمندان و مدیران سیستم که مسئول اجرای وظایف مرتبط با DNS هستند، منتشر شده است.

- **NIST 800-92: Guide to Computer Security Log Management, (2006)**

هدف این سند کمک به سازمان‌ها در درک الزاماتی برای مدیریت رویدادهای امنیتی می‌با شد. سند فوق یک راهنمای کاربردی را برای توسعه، پیاده سازی و حفاظت موثر از روش‌های مدیریت وقایع در سراسر یک سازمان فراهم می‌نماید. راهنمای این سند همچنین حوزه‌های مختلفی از جمله ایجاد زیرساخت‌های مدیریت وقایع و توسعه و اجرای فرآیندهای مدیریت وقایع را در سراسر یک سازمان پوشش می‌دهد. سند موجود فناوری‌های مدیریت وقایع را از یک دیدگاه سطح بالا ارایه می‌دهد و یک راهنمای گام به گام برای پیاده‌سازی یا استفاده از فناوری‌های مدیریت وقایع نیست.

- **NIST SP 800-94: Guide to Intrusion Detection and Prevention Systems (IDPS), Rev 1, (2012)**

هدف این سند کمک به سازمان‌ها در فهم فناوری‌های سیستم پیشگیری از نفوذ[4] و سیستم تشخیص نفوذ[5] و همچنین طراحی، پیاده‌سازی، پیکربندی، امن‌سازی، پایش و حفاظت این سیستم‌ها می‌باشد. این سند یک راهنمای کاربردی را برای هر چهار کلاس محصولات IDPS ازجمله مبتنی بر شبکه، بی سیم، تحلیل مبتنی بر شبکه و مبتنی بر میزبان ارایه می‌دهد. این سند مروری نیز از فناوری‌های مکمل که می‌توانند نفوذهایی به مواردی مانند اطلاعات امنیتی و نرم‌افزار مدیریت وقایع و ابزارهای تحلیل جرم‌یابی شبکه تشخیص دهند را ارایه می‌دهد. همچنین بر روی راه حل‌های IDPS سازمانی تمرکز می‌نماید اما بسیاری از اطلاعات سند با ساختارهای IDPS کوچک و تک‌ایستا[6] قابل اجرا می‌باشد. این سند جایگزین استاندارد NIST 800-31 شده است.

- **NIST SP 800-95: Guide to Secure Web Services, (2007)**

این سند به دنبال کمک به سازمان‌ها در درک چالش‌های یکپارچه‌سازی روش‌های امنیت اطلاعات در طراحی معماری سرویس‌گرا[7] و توسعه براساس سرویس‌های وب می‌باشد. این سند راهنمایی را نیز برای استانداردهای کاربردی سرویس‌های وب فراهم می‌نماید. همچنین اطلاعاتی که به طور وسیعی مستقل از بسترهای سخت‌افزاری ویژه، سیستم‌های عامل و برنامه‌های کاربردی هستند را ارایه می‌دهد. مکانیسم‌های امنیتی مکمل مانند تجهیزات امنیتی محیطی در خارج از حیطه این سند هستند.

- **NIST SP 800-97: Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11i, (2007)**

این سند به دنبال کمک به سازمان‌ها در درک، انتخاب و پیاده سازی فناوری‌هایی براساس استاندارد 802.11i (IEEE) می‌باشد که بخشی از خانواده استاندارد شبکه بی سیم IEEE 802.11 است. سند

---

[4] intrusion prevention system

[5] intrusion detection system

[6] standalone

[7] service-oriented architecture

مذکور ویژگی‌های امنیتی و قابلیت‌های مرتبط با استاندارد IEEE 802.11i را از طریق چارچوب آن برای شبکه‌های امن مستحکم یا RSN[8] توضیح می‌دهد و راهنمای کاملی به منظور برنامه‌ریزی و توسعه RSNها ارایه می‌دهد. این سند درباره سنجش‌های امنیتی IEEE 802.11 و نقطه‌ضعف‌های آن‌ها نیز بحث می‌کند.

- **NIST SP 800-113: Guide to SSL VPNs, (2008)**

این سند به دنبال کمک به سازمان‌ها در فهم فناوری‌های SSL VPN و طراحی، پیاده‌سازی، پیکربندی، امن‌سازی، پایش و نگهداری راه حل‌های این فناوری‌ها می‌باشد. این سند یک رویکرد مرحله‌ای را برای برنامه‌ریزی و پیاده‌سازی فناوری‌های SSL VPN فراهم می‌کند که می‌تواند در دستیابی به توسعه موفق این فناوری‌ها کمک نماید. این سند سنجشی را با سایر فناوری‌های مشابه مانند شبکه خصوصی مجازی مبتنی‌بر IPsec و سایر راه‌حل‌های VPN ارایه می‌دهد.

- **NIST 800-119: Guidelines for the Secure Deployment of IPv6, (2010)** (

هدف فراهم نمودن راهنمای امنیت اطلاعات برای سازمان‌هایی است که در حال برنامه‌ریزی برای توسعه فناوری‌های IPv6 و یا به طور ساده‌تر به دنبال فهم بهتری از این پروتکل می‌باشند. محدوده این نشریه شامل پروتکل IPv6 و مشخصات آن می‌باشد. ملاحظات امنیتی مرتبط با IPv6 با تاکید بر نگرانی‌های امنیتی مرتبط با توسعه آن بیان می‌شود. سند مذکور همچنین شامل راهنمایی عمومی درباره برنامه‌ریزی یکپارچه و توسعه امن IPv6 می‌باشد.

- **NIST SP 800-120: Recommendation for EAP Methods Used in Wireless Network Access Authentication, (2009)**

این سند یکسری از نیازمندی‌های امنیتی اصلی را برای متدهای پروتکل احراز هویت توسعه‌پذیر[9] برای احراز هویت دسترسی بی‌سیم و ایجاد کلید، در هنگام به کارگیری توسط دولت فدرال ایالات متحده بیان

---

[8] Robust Security Network
[9] Extensible Authentication Protocol

می‌کند. این توصیه‌نامه اعتبار سنجی تعدادی از متدهای پروتکل EAP انتخاب شده را به منظور تشریح نیازمندی‌ها بررسی می‌کند. در بخش ۴ این توصیه‌نامه معرفی پروتکل EAP و روش‌های آن، بخش ۵ مباحث آسیب‌پذیری‌های امنیتی آن‌ها و نیازمندی‌های امنیتی در بخش ۸ و۹ ارایه شده است.

- **NIST SP 800-123: Guide to General Server Security, (2008)**

هدف این سند کمک به سازمان‌ها جهت درک فعالیت‌های اصلی انجام شده به منظور امن‌سازی و حفظ امنیت سرویس‌دهنده‌هایی است که سرویس‌هایی را بر روی ارتباطات شبکه به عنوان یک عمل اصلی ارایه می‌دهند. میزبان‌هایی که تصادفا یک یا چند سرویس را به منظور نگهداری یا در دسترس پذیری، مانند سرویس دسترسی راه دور جهت عیب‌یابی ارایه می‌دهند، در این سند در نظر گرفته نمی شوند. این سند ضرورت نیاز به امن سازی سرویس‌دهنده‌ها را مورد بررسی قرار داده و توصیه‌هایی را برای انتخاب، پیاده‌سازی و حفظ کنترل‌های امنیتی لازم ارایه می‌دهد، همچنین سرویس‌دهنده‌های متداولی که از سیستم عامل‌های عمومی مانند یونیکس، لینوکس و ویندوز استفاده می‌کنند را پوشش می‌دهد. بیشتر توصیه‌ها در این نشریه ممکن است برای سرویس‌دهنده‌هایی مناسب باشد که از سیستم‌عامل‌های اختصاصی استفاده کرده یا بر روی برنامه‌های ویژه‌ای اجرا می شوند، اما سایر دستورالعمل‌های این سند ممکن است قابل پیاده‌سازی نباشد و یا عواقب ناخواسته‌ای داشته باشند، بنابراین این چنین سرویس‌دهنده‌هایی خارج از دامنه این سند می‌باشد. دیگر انواع سرویس‌دهنده‌ها مانند سرویس‌دهنده‌های مجازی و بسیار تخصصی، تجهیزات زیر ساخت امنیتی اختصاصی (مانند دیواره‌های آتش و سیستم‌های تشخیص نفوذ) که نیازهای امنیتی و پیکربندی‌های غیر معمول دارند، خارج از دامنه این نشریه می‌باشد.

بخش‌های مختلف این استاندارد بدین شرح است:

- بخش دوم، شامل اطلاعات پایه درباره سرویس‌دهنده‌ها و ارایه مرور کلی درباره نگرانی‌های امنیتی سرویس‌دهنده و همچنین معرفی مراحل بالاتر امن‌سازی سرویس‌دهنده
- بخش سوم، بحث درباره برنامه‌ریزی امنیتی و مدیریت سرویس‌دهنده‌ها
- بخش چهارم، ارایه مروری از امن‌سازی سیستم عامل‌های سرویس‌دهنده

- بخش پنجم، بحث فعالیت‌های مورد نیاز برای نصب امنیتی و پیکربندی نرم‌افزار سرویس‌دهنده مانند نرم‌افزار سرویس‌دهنده وب و ایمیل
- بخش ششم، دستورالعمل‌هایی برای نگهداری امنیت سرویس‌دهنده

➢ **NIST SP 800-125B: Secure Virtual Network Configuration for Virtual Machine (VM) Protection, (2016)**

این سند درباره چهار حوزه پیکربندی شبکه مجازی از جمله بخش‌بندی شبکه، افزونگی مسیر شبکه[10]، کنترل ترافیک با استفاده از دیواره آتش و پایش ترافیک ماشین مجازی می‌باشد که از توجه خاصی به لحاظ امنیتی برخوردارند. بسیاری از تنظیمات پیکربندی در هر یک از این حوزه‌ها، مزایا و معایب مختلفی دارند. هدف این سند تحلیل این مزایا و معایب از نقطه نظر امنیتی بوده و توصیه‌هایی را برای سازمان‌ها جهت استفاده از تنظیمات پیکربندی فراهم می‌کند. این سند تنها حفاظت‌های سطح شبکه را برای ماشین‌های مجازی نمایش می‌دهد. دو حوزه دیگری که سازمان‌ها نیاز دارند تا تضمین همپوشانی امنیت ماشین مجازی و برنامه‌های مستقر شده در آن‌ها فراهم گردد، حفاظت سطح میزبان و داده ماشین مجازی می‌باشد که این حوزه‌ها خارج از محدوده این سند می‌باشند.

➢ **NIST SP 800-128: Guide for Security-Focused Configuration Management of Information Systems, (2011)**

اجزای یک سیستم اطلاعاتی شامل پردازنده مرکزی، ایستگاه‌های کاری، سرویس‌دهنده‌ها از جمله پایگاه داده، پست الکترونیک، احراز هویت، وب، پروکسی، فایل و نام دامنه، اجزای شبکه از جمله دیواره آتش، مسیریاب‌ها، دروازه‌های پیش‌فرض، نقاط دسترسی بی‌سیم، تجهیزات شبکه، سنسور، سیستم‌عامل‌ها، میان‌افزار و برنامه‌های کاربردی می‌باشد که همه این اجزا بایستی شبکه‌بندی، پیکربندی و مدیریت شوند.

مدیریت پیکربندی سیستم نیز یک حداقل نیاز امنیتی تعریف شده در استاندارد FIBS 200 می‌باشد و استاندارد NIST SP 800-537 کنترل‌های امنیتی را که از این نیازمندی‌ها پشتیبانی می‌کند، تعریف

---

[10] Network Path Redundancy

می‌نماید. این سند راهنمایی را برای پیاده‌سازی خانواده مدیریت پیکربندی کنترل‌های امنیتی تعریف شده در استاندارد NIST SP 800-53 فراهم می‌کند و همچنین شامل دستورالعمل‌هایی برای کنترل‌های امنیتی استاندارد NIST SP 800-53 است که مرتبط با مدیریت پیکربندی معماری سیستم اطلاعاتی و اجزای وابسته برای پردازش امن، ذخیره سازی و انتقال اطلاعات می‌باشند. مدیریت پیکربندی یک فرآیند مهم برای ایجاد و نگهداری پیکربندی سیستم اطلاعاتی امن می‌باشد و پشتیبانی عمده‌ای از مدیریت ریسک‌های امنیتی در سیستم اطلاعاتی را فراهم می‌آورد.

- **NIST SP 800-127: Guide to Securing WiMAX Wireless Communications, (2010)**

هدف این سند فراهم نمودن اطلاعاتی برای سازمان‌ها در خصوص قابلیت‌های امنیتی ارتباطات بی‌سیم با استفاده از شبکه‌های وایمکس و فراهم نمودن توصیه‌هایی برای استفاده از این قابلیت‌ها می‌باشد. فناوری وایمکس یک تکنولوژی شبکه بی‌سیم کلان شهری[11] براساس استاندارد IEEE 802.16 می‌باشد و برای اهداف گوناگونی از جمله دسترسی پهن باند آخرین مایل ثابت[12]، تماس مستقیم بی‌سیم طیف وسیع، و فناوری لایه دسترسی برای عامل مشترکان بی‌سیم تلفن همراه در شبکه‌های ارتباطی و ... به‌کار می‌رود. محدوده این سند به امنیت لینک ارتباطی[13] وایمکس و تجهیزات کاربر از جمله سرویس‌های امنیتی برای احراز هویت تجهیزات و کاربر، محرمانگی داده، صحت داده محدود می شود و مشخصات سیستم شبکه وایمکس را پوشش نمی‌دهد. این نشریه راهنمایی را به منظور پیاده‌سازی سیستم‌های وایمکس فراهم می‌نماید.

- **NIST 800-150: Guide to Cyber Threat Information Sharing, (2016)**

این سند راهنمایی برای کمک به سازمان‌ها به منظور مبادله اطلاعات تهدید سایبری می‌باشد. این سند، اشتراک‌گذاری اطلاعات تهدید سایبری داخل یک سازمان، استفاده از اطلاعات تهدید سایبری دریافت شده از منابع خارجی و تولید اطلاعات تهدید سایبری که می‌تواند با سایر سازمان‌ها به اشتراک

---

[11] wireless metropolitan area network

[12] fixed last-mile broadband access

[13] Air interface

گذا شته شود را پو شش می‌دهد و همچنین ملاحظات خا صی را برای جوامع به ا شتراک‌گذاری اطلاعات ارایه می‌دهد.

- **NIST SP 800-153: Guidelines for Securing Wireless Local Area Networks (WLANs), (2012)**

هدف این ســـند فراهم نمودن توصـــیه‌هایی برای بهبود پیکربندی امنیتی و پایش شـــبکه‌های محلی بی‌ســـیم و تجهیزات متصـــل به این شـــبکه‌ها می‌باشـــد. محدوده این ســـند شـــبکه‌های بی‌ســـیم و امکانات طبقه‌بندی نشده در محدوده شبکه‌های بی سیم طبقه‌بندی نشده می‌باشد. مطالب ارایه شده در این سند نیاز به پیگیری توصیه‌ها در دیگر اسناد NIST از جمله SP 800-48 و SP 800-97 را از بین نمی‌برند و چنانچه تضادی بین توصیه‌نامه‌ها در این سند و دیگر نشریات بی‌سیم NIST وجود داشته باشد، باید گفت که توصیه‌نامه موجود در این سند در اولویت قرار دارد.

- **NIST SP 800-175A: Guideline for Using Cryptographic Standards in the Federal Government: Directives, Mandates and Policies, (2016)**

این نشریه شامل راهنمایی‌های جهت ا ستفاده از رمزنگاری و ا ستانداردهای رمزنگاری NIST تو سط دولت فدرال برای حفاظت از اطلاعات حساس دیجیتالی و طبقه‌بندی نشده در هنگام انتقال و ذخیره‌سازی می‌با شد و راهنمایی را جهت شنا سایی الزامات مورد نیاز برای رمزنگاری فراهم می‌نماید. این سند شامل خلا صه‌ای از قوانین و مقررات مربوط به حفاظت از اطلاعات حساس دولت فدرال، راهنمایی در مورد رفتار ارزیابی ریســـک به منظور تعیین آنچه که نیاز به محافظت داشـــته و بهترین روش برای محافظت از آن اطلاعات و بحث درباره اسناد مرتبط با امنیت از جمله اسناد رویه و سیاست‌های گوناگون می‌باشد.

- **NIST SP 800-175B: Guideline for Using Cryptographic Standards in the Federal Government: Cryptographic Mechanisms, (2016)**

این سند درباره متدها و سرویس‌های موجود رمزنگاری برای حفاظت از اطلاعات حساس دولت فدرال بوده و مروری از ا ستانداردهای رمزنگاری NIST را فراهم می‌نماید. یک متخصص تهیه نیازمندی‌ها که در

حال تو سعه یک سیستم، شبکه یا سرویس می‌با شد نیاز به متدهای رمزنگاری به منظور انجام عملیات امنیتی دارد.

- **NIST SP 800-184: Guide for Cybersecurity Event Recovery, (2016)**

هدف این سند کمک به سازمان‌ها به شیوه‌ای مستقل از تکنولوژی در بهبود برنامه بازیابی وقایع سایبری، فرآیندها و رویه‌های آن‌ها با هدف بازگشت سریع‌تر عملیات نرمال و طبیعی خود می‌باشد.

این سند جایگزین دستورالعمل‌های موجود فدرال در رابطه با فرآیند پاسخگویی به حوادث با ارایه اطلاعات عملی به صورت خاص در آماده سازی برای بازیابی وقایع سایبری و د ستیابی به بهبود م ستمر قابلیت‌های بازیابی نمی‌شود.

محدوده این سند موسسات فدرال ایالات متحده می‌باشد و اطلاعات ارایه شده بایستی برای هر سازمان در هر بخش صنعتی که قصد دارد یک رویکرد فراگیر و انعطاف‌پذیرتر جهت بازیابی اطلاعات داشته باشد، مفید باشد. همچنین این سند راهنمایی را به سازمان‌ها در برنامه‌ریزی و آماده‌سازی جهت بازیابی یک رویداد سایبری و یکپارچه سازی فرآیندها و شیوه‌ها در برنامه‌ریزی مدیریت ریسک سازمان ارایه می‌کند ولی به منظور پاسخگویی سازمان به یک رویداد سایبری فعال به‌کار نمی‌رود، اما به عنوان یک راهنمایی به منظور توسعه برنامه بازیابی خود به شکل راهکارهای سفارشی پیش از رویداد فعال استفاده می‌شود.

- **SP 800-171: Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations, Rev 1, (2016)**

حفاظت از اطلاعات غیرمحرمانه طبقه‌بندی نشده در سازمان‌ها و سیستم‌های اطلاعاتی غیر فدرال از اهمیت فوق‌العاده‌ای نسبت به موسسات فدرال برخوردارند و می‌توانند قابلیت دولت فدرال را تحت تاثیر مستقیم خود قرار دهند تا بصورت موفقیت آمیز ماموریت تعیین شده و عملیات کسب و کار را انجام دهد.

هدف این نشریه فراهم نمودن موسسات فدرال با نیازمندی‌های توصیه شده برای حفاظت از محرمانگی اطلاعات طبقه‌بندی نشده کنترل شده یا CUI[۱۴] می‌باشد.

از این استاندارد یک ویرایش در سال ۲۰۱۶ نیز منتشر شده است و دارای دو بخش کلی می‌باشد: درفصل دوم آن یکسری فرضیات و متدها برای توسعه نیازمندی‌های امنیتی CUI، قالب و ساختار نیازمندی‌ها و در فصل سوم ۱۴ خانواده از انواع نیازمندی‌های امنیتی حفاظت از محرمانگی CUI در سیستم‌ها و سازمان‌های غیر فدرال بیان می‌شوند.

- **FIPS 199: Standards for Security Categorization of Federal Information and Information Systems, (2004)**

این سند، استانداردهایی را برای طبقه‌بندی امنیت اطلاعات و سیستم‌های اطلاعاتی ایجاد می‌کند. استانداردهای طبقه‌بندی امنیتی برای اطلاعات و سیستم‌های اطلاعاتی یک چارچوب مرسوم را فراهم می‌نمایند و برای دولت فدرال مواردی مانند مدیریت موثر و نظارت بر برنامه‌های امنیت اطلاعات، کفایت و اثربخشی سیاست‌های امنیت اطلاعات، روش‌ها و شیوه‌ها را توسعه می‌دهند.

- **FIPS 200: Minimum Security Requirements for Federal Information and Information Systems, (2006)**

این ا ستاندارد، حداقل الزامات امنیتی برای اطلاعات و سی ستم‌های اطلاعاتی که سازمان‌های اجرایی دولت فدرال را پشتیبانی می‌کنند و همچنین یک فرآیند مبتنی بر ریسک برای انتخاب کنترل‌های امنیتی مورد نیاز جهت برقراری حداقل نیازمندی‌های امنیتی را پ شتیبانی می‌نماید. این ا ستاندارد از طریق ایجاد حداقل سطوح لازم برای امنیت اطلاعات و تسهیل یک رویکرد سازگارتر، قیاس‌پذیر و قابل تکرار برای انتخاب و مشخص نمودن کنترل‌های امنیتی برای سیستم‌های اطلاعاتی که با حداقل نیازمندی‌های

[14] Controlled Unclassified Information

امنیتی سازگار باشند، توسعه، پیاده‌سازی و استفاده از سیستم‌های اطلاعاتی امن‌تر در داخل دولت فدرال را ترویج می‌دهد.

- **FIPS 140-2: Security Requirements for Cryptographic Modules, (2001)**

این استاندارد نیازمندی‌های خاص ماژول رمزنگاری را مشخص می‌کند و چهار سطح افزایش کیفی (از سطح یک تا چهار) برای پوشش طیف گسترده‌ای از قابلیت‌های برنامه و محیط ارایه می‌دهد. این سند، نیازمندی‌های امنیتی مناطقی را که در رابطه با طراحی و اجرای ماژول رمزنگاری است را پوشش می‌دهد که شامل مشخصات ماژول، پورت‌ها و رابط‌ها، نقش‌ها، سرویس‌ها، احرازهویت، مدل وضعیت محدود، امنیت فیزیکی، محیط عملیاتی، مدیریت کلید رمزنگاری، رابط مغناطیسی، مطابقت مغناطیسی (EMI/EMC)، خودآزمایی و طراحی مطمئن می‌شود. همچنین این استاندارد تعیین می‌کند که توسعه‌دهندگان ماژول‌های رمزنگاری و فروشندگان آن‌ها به منظور کاهش حملات به چه کنترل‌های امنیتی خاصی نیاز دارند.

- **ISO/IEC 27033: ISO/IEC 27033:2010+ Information technology — Security techniques — Network security, (2010)**

هدف این استاندارد فراهم نمودن راهنمایی جامع براساس جنبه‌های امنیتی مدیریت، عملیات و استفاده از شبکه‌های سیستم اطلاعاتی و ارتباط داخلی آن‌ها می‌باشد. همچنین این استاندارد راهنمایی جامع را برای پیاده‌سازی کنترل‌های امنیتی معرفی شده در استاندارد ISO/IEC 27002 ارایه می‌دهد. این مورد با امنیت تجهیزات شبکه و مدیریت امنیت آن‌ها، سرویس‌ها/برنامه‌های کاربردی و کاربران شبکه علاوه بر امنیت اطلاعات قابل انتقال از طریق لینک‌های ارتباطی اعمال می‌شود. این استاندارد شامل بخش‌های زیر است:

- بخش اول: مرور و مفاهیم امنیت شبکه
- بخش دوم: راهنمایی برای طراحی و پیاده سازی امنیت شبکه
- بخش سوم: مرجع سناریوهای شبکه، ریسک‌ها و تکنیک‌های طراحی و کنترل مسائل مهم

- بخش چهارم: تامین امنیت ارتباطات بین شبکه با استفاده از Gatewayهای امن
- بخش پنجم: تامین امنیت برای شبکه‌های VPN
- بخش ششم: دسترسی امن شبکه‌های IP بی‌سیم

➢ **ISO/IEC 27035: Information technology — Security techniques — Information security incident management, (2016)**

مدیریت حوادث به طور موثر دربرگیرنده تشخیص و تصحیح کنترل‌های طراحی شده به منظور تشخیص و پاسخگویی به رویدادها و حوادث، حداقل‌سازی تاثیرات ناسازگار، گردآوری شواهد جرم‌یابی و غیره می‌باشد. حوادث امنیت اطلاعات به طور عادی دربرگیرنده استخراج آسیب‌پذیری‌های تشخیص داده نشده و یا کنترل‌نشده می‌باشد زیرا مدیریت آسیب‌پذیری بخشی پیشگیرانه و عملی اصلاحی است. هدف این استاندارد پوشش فرآیندهایی برای مدیریت رویدادهای امنیتی اطلاعات، حوادث و آسیب‌پذیری‌هاست. این استاندارد بخش مدیریت حوادث امنیت اطلاعات از استاندارد ISO/IEC 27002 را توسعه می‌دهد و در بخش‌های زیر تدوین شده است:

- بخش اول: اصول مدیریت حوادث
- بخش دوم: راهنمایی به منظور برنامه‌ریزی و آماده‌سازی برای پاسخگویی به حوادث
- بخش سوم: راهنمایی برای عملیات پاسخگویی به حوادث (پیش نویس)

➢ **ISO/IEC 27039: Information technology — Security techniques — Selection, deployment and operation of intrusion detection and prevention systems (IDPS), (2015)**

این استاندارد ویرایش جدیدی از استاندارد ISO/IEC 18043 می‌باشد. سیستم‌های تشخیص نفوذ سیستم‌های خودکاری برای شناسایی حملات و یا نفوذهای وارد شده به یک شبکه یا سیستم، توسط هکر بوده و به منظور تولید هشدار به کار می‌روند. سیستم‌های پیشگیری از نفوذ سیستم‌های IPS به طور خودکار به نوع خاصی از حملات شناخته شده برای مثال با بستن یکسری درگاه‌های خاص شبکه از طریق دیواره آتش به منظور بلوک کردن ترافیک هکر شناسایی شده پاسخ می‌دهند. هدف این استاندارد کمک

به سازمان‌ها به منظور استقرار سیستم تشخیص و پیشگیری از نفوذ می‌باشد و انتخاب، استقرار و عملیات IDPS را بررسی می‌کند. بخش‌های کلیدی استاندارد عبارتند از:

- انتخاب IDPS: انواع مختلف IDPS، ابزارهای مکمل
- استقرار IDPS
- عملیات IDPS

➢ **RFC 4130: MIME-Based Secure Peer-to-Peer Business Data Interchange Using HTTP, Applicability Statement 2 (AS2), (2005)**

این سند یک بیانیه کاربردی را ارایه می‌کند که نحوه مبادله داده‌های کسب و کار ساخت یافته به صورت امن را با استفاده از پروتکل انتقال HTTP به جای پروتکل SMTP شرح می‌دهد. بیانیه کاربرد برای پروتکل SMTP در استاندارد RFC 3335 وجود دارد. داده‌های کسب و کار ساخت یافته ممکن است به صورت XML، تبادل داده الکترونیک[۱۵] در فرمت X12 موسسه استانداردهای ملی آمریکا یا EDI در فرمت سازمان ملل متحد برای مدیریت، تجارت و حمل و نقل و یا سایر فرمت‌های داده ساخت یافته باشند. این سند توسعه یافته استاندارد RFC 1767 به منظور مشخص نمودن مجموعه جامعی از ویژگی‌های امنیتی داده، به طور خاص محرمانگی داده‌ها، اعتبار-صحت داده‌ها، عدم انکار مبدا و عدم انکار دریافت در سراسر پروتکل HTTP می‌باشد.

همچنین هدف آن معرفی MIME EDI و ارایه مشخصات آن، تضمین قابلیت همکاری میان عامل‌های کاربر B2B EC[۱۶]، با استناد به برخی یا کلیه ویژگی‌های امنیتی مورد انتظار می‌باشد. این نشریه محدود به استفاده از EDI محض نمی‌شود، بلکه در هر برنامه کاربردی تجارت الکترونیک که اطلاعات کسب و کار نیاز به تبادل در اینترنت به شیوه‌ای امن دارند، قابل اعمال است.

---

[15] Electronic Data Interchange

[16] business-to-business, electronic commerce

- **RFC 4033 :DNS Security Introduction and Requirements, (2005)**

ضمیمه‌های امنیتی DNS یک مجموعه از اسناد IETF می‌باشد که برای تامین امنیت برخی از اطلاعات آماده شده توسط DNS، در پروتکل اینترنت IP شبکه‌ها استفاده می‌شود. سند پیش رو درباره سرویس‌هایی است که ضمیمه‌های امنیتی سیستم نام دامنه[17] را می‌توانند فراهم کنند. DNSSEC، احرازهویت منبع داده و صحت داده را به DNS می‌افزایند. این سند این ضمیمه‌ها را معرفی نموده و همچنین قابلیت‌ها و محدودیت‌های آن‌ها را نیز شرح می‌دهد.

در انتها این سند ارتباط متقابل اسنادی که به طور جامع DNSSEC را توصیف می‌کنند را تشریح می‌کند که این سند و اسناد مرتبط با آن مانند RFC 4034 و RFC 4035 تعاریف موجود در RFC 2535 را به روزرسانی و اصلاح می‌نمایند.

- **RFC 4034: Resource Records for the DNS Security Extensions, (2005)**

این نشریه بخشی از خانواده نشریات DNSSEC می‌باشد. ضمیمه‌های امنیتی DNS مجموعه‌ای از اصلاحات پروتکل و رکوردهای منبع هستند که احراز هویت منبع را برای DNS فراهم می‌کنند. این سند کلید عمومی، هیئت امضاکننده[18]، امضای دیجیتال رکورد منبع و انکار وجود رکوردهای منبع تصدیق شده را تعریف می‌کند. جزئیات هدف و قالب هر رکورد تشریح گردیده و یک نمونه از هر رکورد منبع بیان شده است.

- **RFC 4035: Protocol Modifications for the DNS Security Extensions, (2005)**

این نشریه بخشی از خانواده نشریات DNSSEC می‌باشد. ضمیمه‌های امنیت DNS مجموعه‌ای از اصلاحات پروتکل و رکوردهای منابع جدید هستند که احراز هویت منابع داده و صحت داده را به DNS می‌افزایند. این سند اصلاحات پروتکل DNSSEC را توصیف می‌کند. این سند مفهوم یک منطقه امضا

---

[17] Domain Name System Security Extensions

[18] Delegation signer

شده[19] را همراه با الزاماتی برای حل کردن مسایل با استفاده از DNSSEC تعریف می‌کند. این روش‌ها به حل کننده امنیتی، امکان احراز هویت رکوردهای منبع DNS و نشانه‌های خطای DNS معتبر را می‌دهد. بخش ۲ این سند مفاهیم منطقه امضا شده را تعریف نموده و فهرستی از نیازمندی‌ها را برای امضای منطقه مشخص می‌کند. بخش ۳ اصلاحاتی را برای رفتار سرویس‌دهنده نام معتبر جهت بررسی مناطق امضا شده تشریح می‌کند. بخش ۴ رفتار هویت‌هایی را که شامل عملیات حل کننده امنیتی می‌شوند شرح می‌دهد. در نهایت، بخش ۵ چگونگی استفاده از رکوردهای منبع DNSSEC را به منظور احراز هویت یک پاسخ (واکنش) بیان می‌کند.

- **RFC 4398: Storing Certificates in the Domain Name System (DNS), (2006)**

کلیدهای عمومی غالبا به صورت یک گواهی‌نامه منتشر می‌شوند و معمولا اعتبار آن‌ها به وسیله گواهی‌نامه‌ها و لیست‌های ابطال گواهی‌نامه[20] مربوطه اثبات می شود. یک گواهی‌نامه الحاقی از یک امضای دیجیتال رمزنگاری، یک کلید عمومی، اطلاعات هویت، مجوزدهی و ... می‌باشد. لیست ابطال گواهی‌نامه، لیستی از گواهی‌نامه‌هایی است که ابطال شده‌اند و تمامی اطلاعات ضمنی توسط امضاکننده گواهی‌نامه‌های ابطال شده امضا می‌شوند.

DNSSEC از هر گونه اطلاعات تولید شده توسط DNS محافظت می‌نماید و می‌تواند به منظور راه‌اندازی دیگر سیستم‌های امنیتی به‌کار رود. این استاندارد ذخیره‌سازی رکوردهای گواهی نامه‌های رمزنگاری ذخیره شده در DNS را بررسی می‌کند. بخش دوم این استاندارد، رکورد منبع CERT را برای ذخیره گواهینامه‌ها در DNS، بخش ۳ نام‌های مالک مناسب برای رکوردهای منبع CERT، بخش ۴، ۷ و ۸ به ترتیب کارآیی، امنیت و ملاحظات IANA[21] و بخش ۹ تغییرات این سند را در مقایسه با سند RFC 2538 شرح می‌دهد.

---

[19] signed zone

[20] CRLs

[21] Internet Assigned Numbers Authority

- **RFC 4255: Using DNS to Securely Publish Secure Shell (SSH) Key Fingerprints, (2006)**

این سند یک روش تایید کلیدهای میزبان SSH را با استفاده از DNSSEC شرح داده و یک رکورد منبع DNS جدید، حاوی اثرانگشت کلید SSH را تعریف می‌کند.

در به‌کارگیری اثر انگشت در اتصالات SSH با سرویس‌دهنده در صورتی که کاربر تشخیص دهد که اثر انگشت صحیح بوده و کلید را بپذیرد، کلید به صورت محلی ذخیره شده و جهت تایید برای ادامه اتصالات به‌کار می‌رود، اما ممکن است که کاربر تایید اثر انگشت را خارج از این محدوده انجام دهد و بسیاری از کاربران کلید ارایه شده را بدون هیچگونه بررسی می‌پذیرند. روش تشریح شده در RFC 4255 می‌تواند بررسی خارج از محدوده‌ای را با جستجوی اثر انگشت کلید عمومی سرویس‌دهنده در DNS و به‌کارگیری DNSSEC به منظور تایید جستجو فراهم نماید.

- **RFC 7671: The DNS-Based Authentication of Named Entities (DANE) Protocol: Updates and Operational Guidance, (2015)**

این سند مشخصات بیان شده در سند RFC 6698 را براساس تجربیات حاصل شده از پیاده‌سازی‌های پس از آن، تشریح و به روزرسانی می‌کند و شامل راهنمایی برای مجریان، متصدیان و توسعه‌دهندگان پروتکل که تمایل به استفاده از رکوردهای DANE دارند، می‌باشد. استاندارد RFC 6698 سه فیلد رکورد TLSA را تعریف می‌کند. اولین مورد با ۴ مقدار، دومین مورد با ۲ و سومین با ۳ مقدار ممکن وجود دارند. در نتیجه ۲۴ ترکیب متمایز از انواع رکوردهای TLSA حاصل می‌شود. این سند مجموعه کوچکتری از بهترین ترکیبات فیلدهای استاندارد RFC 6698 را معرفی می‌نماید تا سادگی در طراحی، پیاده‌سازی و استقرار پروتکل ایجاد گردد. این مسئله با راهنمایی استقرار و عملیات در RFC 7671 به روزرسانی شده است.

- **RFC 7513: Source Address Validation Improvement (SAVI) Solution for DHCP, (2015)**

سند RFC 7513 روش‌هایی را برای ایجاد اتصالاتی میان آدرس‌های IP تخصیص داده شده به DHCPv4/DHCPv6 و لنگر متصل‌کننده روی یک دستگاه بهبود اعتبارسنجی آدرس مبدا، ایجاد می‌کند. در بخش ۳ از استاندارد RFC 7039 لنگرهای اتصال اینگونه تعریف شده است: لنگر اتصال ویژگی غیرقابل تغییری است که ممکن است به منظور شناسایی سیستمی‌که تخصیص یک آدرس IP روی آن صورت گرفته، به‌کار رود. اتصالات به منظور شناسایی و فیلتر نمودن بسته‌های تولید شده توسط واسط‌ها با استفاده از آدرس‌های IP مبداء جعلی به‌کار می‌روند. در این روش، این مکانیسم می‌تواند از جعل آدرس IP در شبکه جلوگیری نماید.

- **RFC 7610: DHCPv6-Shield: Protecting against Rogue DHCPv6 Servers, (2015)**

این سند مکانیسمی را برای محافظت میزبان‌های متصل به شبکه‌های سوئیچی در برابر سرویس‌دهنده‌های DHCPv6 متقلب و همچنین بهترین اقدامات برای پیاده‌سازی پوشش محافظ DHCPv6 را ارایه می‌دهد و براساس پالایش بسته‌های DHCPv6 در ابزار لایه ۲ که در آن بسته‌ها دریافت می‌شوند، می‌باشد.

- **RFC 6353: Transport Layer Security (TLS) Transport Model for the Simple Network Management Protocol (SNMP), (2011)**

مدل امنیت انتقال، متدی را برای احراز هویت و رمزنگاری پیام بر روی کانال‌های امنیتی خارجی فراهم می‌کند. دو پروتکل انتقال SSH و TLS/DTLS تعریف شده در این استاندارد استفاده از مشخصات مدل امنیت انتقال را بیان می‌کنند.

- **RFC 7454: BGP Operations and Security**

پروتکل BGP تقریبا به صورت انحصاری به منظور مبادله اطلاعات مسیریابی بین حوزه‌های شبکه به کار می‌رود. با توجه به این طبیعت متمرکز، درک اقدامات امنیتی که بایستی به منظور پیشگیری از اختلالات مسیریابی عمدی یا تصادفی مستقر گردند مهم می‌باشد. این سند اقداماتی از جمله TTL، گزینه احرازهویت TCP و فیلترینگ برنامه کنترل[۲۲] را به منظور حفاظت از نشست‌های BGP تشریح می‌نماید. فیلترینگ برنامه کنترل شامل اعمال سیاست‌های لازم برای فیلتر نمودن هر ترافیکی است که مقصد آن آدرس IP ایک روتر و ... می‌باشد. همچنین اقداماتی را به منظور کنترل بهتر جریان اطلاعات مسیریابی، با استفاده از فیلترینگ پیشوند و خودکارسازی فیلترهای پیشوند، فیلترینگ حداکثر پیشوند، فیلترینگ مسیر سیستم خودکار، کاهش تاثیر مسیر و سایش جامع BGPP تشریح می‌کند. این سند کلیه راهنمایی‌های موجود را خلاصه نموده و به مدیران شبکه در اعمال سیاست‌های منسجم شبکه کمک می‌نماید.

- **RFC 5077: Transport Layer Security (TLS) Session Resumption without Server-Side State, (2008)**

این سند روشی را ارایه می‌دهد که در آن سرویس‌دهنده TLS را قادر می‌سازد تا نشست‌ها را مجددا آغاز نموده و از نگهداری وضعیت نشست هر سرویس‌گیرنده اجتناب نماید. سرویس‌دهنده TLS وضعیت نشست را در یک بلیط کپسوله نموده و آن را به سمت سرویس‌گیرنده ارسال می‌کند. سرویس‌گیرنده متعاقبا می‌تواند با استفاده از بلیط‌هایی که به دست آورده، نشست را مجددا آغاز نماید. این سند تمامی‌ضمیمه‌های TLS تعریف شده در استاندارد RFC 4366 را به‌کار برده و نوع جدیدی از پیام TLS را تعریف می‌کند. این مکانیسم در موارد زیر مفید می‌باشد:

- سرویس‌دهنده‌هایی که تعداد زیادی از تراکنش‌ها را از کاربران مختلف گردآوری می‌کند.
- سرویس‌دهنده‌هایی که تمایل به نشست حافظه کش برای مدت زمان طولانی دارند.

---

[22] control-plane filtering

- توانایی بارگذاری درخواست‌های متعادل در سراسر سرویس‌دهنده
- سرویس‌دهنده تعبیه شده با حافظه کم

➢ **RFC 7301: Transport Layer Security (TLS) Application-Layer Protocol Negotiation Extension, (2014)**

این سند ضمیمه پروتکل TLS را برای مذاکره پروتکل لایه کاربرد در دست تکانی TLS توصیف می‌کند. به طور کلی در این سند پروتکل‌های کاربردی متعددی بر روی یک درگاه UDP یا TCP یکسان پشتیبانی می‌شوند، این ضمیمه به لایه کاربرد امکان مذاکره آن پروتکلی را می‌دهد که در اتصال TLS به‌کار خواهد رفت. به طور فزاینده‌ای پروتکل‌های لایه کاربرد در پروتکل TLS کپسوله می‌شوند. این کپسوله‌سازی برنامه‌ها را جهت استفاده لینک‌های ارتباطی امن و موجود که در حال حاضر روی درگاه ۴۴۳(HTTPS) ارایه می‌شوند، در سراسر زیرساخت IP قدرتمند می‌نماید. هنگامی‌که پروتکل‌های کاربردی متعددی بر روی یک شماره درگاه طرف سرویس‌دهنده مانند ۴۴۳ پشتیبانی می‌شوند، سرویس‌دهنده و مشتری نیاز به مذاکره یک پروتکل کاربردی برای استفاده در هر اتصال دارند که این مذاکره بدون نیاز به افزودن رفت و برگشت‌های شبکه میان سرویس‌دهنده و مشتری به انجام می‌رسد.

➢ **RFC 6242: Using the NETCONF Protocol over Secure Shell (SSH), (2011)**

پروتکل NETCONF یک پروتکل مبتنی بر XML است که برای مدیریت پیکربندی تجهیزات شبکه استفاده می‌شود. NETCONF مستقل از لایه انتقال و نشست تعریف می‌شود تا امکان نگاشت به پروتکل‌های متعدد لایه انتقال یا نشست فراهم شود. این سند چگونگی کاربرد پروتکل NETCONF در نشست SSH با استفاده از پروتکل اتصال SSH (RFC 4254) روی پروتکل انتقال SSH (RFC 4253) را تعریف می‌کند. این نگاشت این امکان را می‌دهد که پروتکل NETCONF از طریق یک نشست پوسته امن، توسط یک کاربر یا نرم‌افزار قابل اجرا باشد. این انتقال می‌تواند برای هر نوع پیام NETCONF به‌کار رود.

- **ETSI TS 133 220: DIGITAL CELLULAR TELECOMMUNICATIONS SYSTEM (PHASE 2+) (GSM)/ UNIVERSAL MOBILE TELECOMMUNICATIONS SYSTEM (UMTS)/ LTE/ GENERIC AUTHENTICATION ARCHITECTURE (GAA)/ GENERIC BOOTSTRAPPING ARCHITECTURE (GBA), (2016)**

این سند به توصیف ویژگی‌ها و مکانیزم‌های امنیتی جهت راه‌اندازی[23] مکانیزم احرازهویت و توافق کلید برای امنیت نرم‌افزار می‌پردازد. نرم‌افزارهای منتخب برای استفاده از این مکانیزم راه‌اندازی شامل توزیع گواهی‌نامه مشترک TS 3.221 می‌باشد، اما محدود به این نیز نمی‌شود. گواهینامه‌های مشترک[24] از سرویس‌هایی که متعلق به همکاران اپراتور تلفن همراه هستند همانند سرویس‌هایی که توسط اپراتور موبایل ارایه می‌شود پشتیبانی می‌کنند.

محدوده این مشخصات شامل توابع راه‌انداز عمومی، یک مرور کلی بر معماری و روش دقیقی درخصوص چگونگی راه‌اندازی گواهی‌نامه می‌باشد.

- **ETSI TS 118 508: Analysis of Security Solutions for the oneM2M System, (2014)**

سند حاضر برای ایجاد درک مشترکی از امنیت در سیستم‌های oneM2M می‌باشد. برای رسیدن به این امر، سرویس‌های امنیتی، تهدیدات تجزیه و تحلیل شده و نیازمندی‌های امنیتی در این سیستم‌ها شناسایی و از موارد کاربردی استخراج گشته است. علاوه بر این سند حاضر ارتباط مکانیزم‌های امنیتی به معماری این سیستم‌ها را نیز مطرح می‌کند. همچنین روش‌ها و مکانیزم‌های امنیتی مناسب در آن تعریف شده است.

- **ETSI EN 300 175-7: Digital Enhanced Cordless Telecommunications (DECT)/Common Interface (CI)/ Part 7: Security features, (2015)**

---

[23] bootstrap

[24] Subscriber certificates

این سند معماری امنیتی، انواع الگوریتم‌های رمزنگاری مورد نیاز، روش‌هایی که آن‌ها در آن مورد استفاده قرار می‌گیرند و الزامات موردنیاز برای یکپارچه‌سازی ویژگی‌های امنیتی ارایه شده با معماری ارتباطات پیشرفته بی‌سیم و دیجیتال (DECT)[۲۵] رابط مشترک (CI)[۲۶] را مشخص نموده و نحوه مدیریت ویژگی‌ها را شرح می‌دهد.

- **IEEE 2600-2008: IEEE Standard for Information Technology: Hardcopy Device and System Security, (2010)**

این استاندارد الزامات امنیتی (تمام جنبه‌های امنیتی ازجمله احرازهویت، مجوزدهی، حفظ حریم خصوصی، صحت، مدیریت دستگاه، امنیت فیزیکی و امنیت اطلاعات و ...) را برای تولیدکنندگان، کاربران و سایر افراد برای انتخاب، نصب و راه‌اندازی، پیکربندی و استفاده از دستگاه‌های چاپی و سیستم‌ها از جمله پرینترها، دستگاه‌های کپی و دستگاه‌های چندمنظوره تعریف می‌کند. این استاندارد مخاطرات امنیتی را برای این دستگاه‌های چاپی و سیستم‌ها مشخص کرده و تولیدکنندگان و توسعه‌دهندگان نرم‌افزار را برای گنجاندن قابلیت‌های امنیتی مناسب در دستگاه‌ها و سیستم‌های خود، راهنمایی می‌کند و کاربران را در راه‌های مناسب برای استفاده از این قابلیت‌های امنیتی آموزش می‌دهد.

- **RFC 5246: The Transport Layer Security (TLS) Protocol, (2008)**

این سند نسخه ۱,۲ از پروتکل امنیت لایه انتقال[۲۷] را مشخص می‌کند. پروتکل TLS ارتباطات امن را در سراسر اینترنت فراهم می‌کند. هدف اصلی از این پروتکل فراهم نمودن حریم خصوصی و صحت داده

---

[25] Digital Enhanced Cordless Telecommunications

[26] Common Interface

[۲۷] Transport Layer Security protocol

بین دو برنامه کاربردی در حال ارتباط می‌باشد. پروتکل از دو لایه تشکیل شده است: پروتکل رکورد TLS و پروتکل دست تکانی TLS. پروتکل اجازه می‌دهد تا برنامه‌های کاربردی سرویس‌گیرنده / سرویس‌دهنده به روشی که برای جلوگیری از استراق سمع، دستکاری، یا جعل پیام طراحی شده است ارتباط برقرار کنند.

- **Authentication and Authorization for Constrained Environments (ACE), (2016)**

برخی از سناریوهای توسعه اینترنت اشیا به یک راه حل مجوزدهی پویا و انعطاف پذیر نیاز دارند که به پیکربندی ایستا لیست‌های کنترل دسترسی وابسته نمی‌باشد.

گروه کاری IETF ACE چگونگی استفاده از OAuth 2.0 به عنوان یک چارچوب مجوزدهی با توسعه‌دهندگان اینترنت اشیا (IoT) را تعریف می کند، در نتیجه یک راه حل امنیتی شناخته شده را برای دستگاه‌های اینترنت اشیا به همراه می‌آورد.

- **ISO/IEC 27000-series: provides a privacy framework, (2016)**

این سری بهترین توصیه‌ها را در رابطه با مدیریت امنیت اطلاعات، ریسک‌ها و کنترل‌ها در زمینه یک سیستم مدیریت امنیت اطلاعات، به طور مشابه در طراحی سیستم‌های مدیریتی برای تضمین کیفیت (سری ایزو ۹۰۰۰) را فراهم می‌کند.

- **Security Services (SAML) TC, (2012)**

زبان نشانه گذاری تاکید امنیتی (SAML) توسط کمیته فنی خدمات امنیتی OASIS توسعه یافته است که چارچوبی مبتنی بر XML برای ارتباط ویژگی‌ها و حقوق و احرازهویت کاربر می‌باشد. همانطور که از نام آن پیداست، SAML اجازه می‌دهد نهادهای کسب و کار هویت و ویژگی‌ها و حقوق یک موجودیت (که اغلب یک کاربر انسانی است) درباره موجودیتی دیگر، مانند یک شرکت همکار ویا نرم‌افزار شرکت دیگری تایید کنند.

- **eXtensible Access Control Markup Language (XACML) TC, (2013)**

XACML یک استاندارد سازمان OASIS است که زبان سیاست و زبان درخواست و پاسخ تصمیمات کنترل دسترسی را توصیف می‌کند. زبان سیاست برای توضیح الزامات عمومی کنترل دسترسی استفاده می‌شود و دارای نقاط قابل گسترش برای تعریف توابع جدید، انواع داده‌ها، ترکیب منطقی و غیره... می‌باشد. زبان درخواست و پاسخ اجازه طرح سوال یا انجام ندادن فعالیتی را همراه با تفسیر نتایج می‌دهد. کمیته فنی این استاندارد یک طرح پایهXML را برای نشان دادن سیاست مجوزدهی و حق تعریف می‌کند.

- **ETSI TS 118 103: Security solutions, (2016)**

سند حاضر راه‌حل‌های امنیتی قابل اجرا در سیستم‌های M2M را بررسی نموده و چارچوبی امنیتی را برای این سیستم‌ها ارایه می‌نماید.

- **ISO/IEC 29100:2011 provides a privacy framework, (2011)**

این استاندارد بین المللی یک چارچوب سطح بالا را برای حفاظت از اطلاعات شناسایی شخصی در سیستم‌های فناوری اطلاعات و ارتباطات فراهم می‌کند. این استاندارد جنبه عمومی دارد و جنبه‌های سازمانی، فنی و رویه‌ای را در چارچوب حریم خصوصی کلی جای می‌دهد. چارچوب حریم خصوصی به منظور کمک به سازمان‌ها جهت مشخص نمودن الزامات حفظ حریم خصوصی اطلاعات شناسایی شخصی خود، در یک محیط فناوری اطلاعات و ارتباطات به وسیله موارد ذیل در نظر گرفته شده است:

- مشخص نمودن یک اصطلاح رایج حریم خصوصی
- تعریف بازیگران و نقش‌های آن‌ها در پردازش اطلاعات شناسایی شخصی
- مشخص کردن الزامات حفظ حریم خصوصی
- ارجاع به اصول حریم خصوصی شناخته شده

این استاندارد برای اشخاص حقیقی و سازمان‌های درگیر در تعیین، تهیه، معماری، طراحی، توسعه، تست، حفظ، مدیریت، وسیستم های عملیاتی اطلاعات و سیستم‌های تکنولوژی ارتباطات یا سرویس‌هایی که کنترل‌های حریم خصوصی برای پردازش اطلاعات شناسایی شخصی مورد نیاز است، قابل اجرا است.

- **XML Key Management Specification, (2005)**

این سند پروتکل‌هایی برای توزیع و ثبت کلیدهای عمومی، مناسب با این استاندارد برای امضای XML مشخص می‌کند. این یک استاندارد دو بخشی است. بخش اول مشخصه پروتکل‌ها و سرویس‌های XKMS را پوشش می‌دهد. بخش دوم توصیه‌های W3C برای مشخصات مدیریت کلید (XKMS Version ۲,۰) اتصالات پروتکل مختلف با خصوصیات امنیتی برای مشخصه مدیریت کلید XML را شرح می‌دهد. این سند مشخصات کلیدی سرویس اطلاعات XML و مشخصات خدمات ثبت نام کلیدی XML را تعریف می‌نماید.

- **IEEE: IEEE Cyber Security for the Smart Grid, (2013)**

این گزارش آسیب‌پذیری‌های امنیتی سایبری موجود در زنجیره ارزش شبکه هوشمند، تلاش‌های انجام شده توسط برخی از کشورها برای کاهش این آسیب‌پذیری‌ها و اقدامات موردنیاز جهت پیشرفت را تفصیل می‌کند. چهار نمونه ازشاخه‌های امنیت سایبری در این گزارش برجسته شده است.