تحقیق ۴: امنیت اینترنت اشیاء (IoT) و زیرساخت‌های حیاتی

۱. مقدمه

در دهه‌های اخیر، جهان شاهد تحول عظیمی در حوزه فناوری بوده است که از آن با عنوان **اینترنت اشیاء (Internet of Things - IoT)** یاد می‌شود. IoT به شبکه‌ای از دستگاه‌های فیزیکی، وسایل نقلیه، لوازم خانگی و سایر اشیاء مجهز به حسگرها، نرم‌افزارها و سایر فناوری‌ها اشاره دارد که امکان اتصال و تبادل داده با سایر دستگاه‌ها و سیستم‌ها را از طریق اینترنت فراهم می‌آورد [1]. از خانه‌های هوشمند و شهرهای هوشمند گرفته تا صنعت ۴.۰ و کشاورزی دقیق، IoT در حال تغییر شکل زندگی روزمره و صنایع مختلف است. همزمان با این گسترش، **زیرساخت‌های حیاتی** که شامل شبکه‌های برق، آب، گاز، حمل و نقل، ارتباطات و سیستم‌های بهداشتی می‌شوند، به طور فزاینده‌ای به فناوری‌های دیجیتال و IoT وابسته شده‌اند. این وابستگی متقابل، در کنار مزایای فراوان، چالش‌های امنیتی منحصر به فرد و پیچیده‌ای را نیز به وجود آورده است.

امنیت در حوزه IoT و زیرساخت‌های حیاتی از اهمیت ویژه‌ای برخوردار است، زیرا هرگونه نقص امنیتی می‌تواند پیامدهای فاجعه‌باری از جمله اختلال در خدمات عمومی، خسارات اقتصادی گسترده، آسیب‌های زیست‌محیطی و حتی تلفات جانی به همراه داشته باشد. این تحقیق به بررسی جامع **تهدیدات امنیتی در اینترنت اشیاء و زیرساخت‌های حیاتی** و ارائه **راهکارهای مؤثر برای افزایش امنیت** در این حوزه‌ها می‌پردازد. هدف اصلی، افزایش آگاهی نسبت به آسیب‌پذیری‌های موجود و ترویج رویکردهای جامع برای حفاظت از این سیستم‌های حیاتی است. در ادامه، ابتدا به تشریح آسیب‌پذیری‌های دستگاه‌های IoT و حملات رایج به آن‌ها خواهیم پرداخت. سپس، تهدیدات سایبری علیه زیرساخت‌های حیاتی و پیامدهای آن‌ها را بررسی کرده و در نهایت، راهکارهای فنی، سازمانی و بین‌المللی برای تقویت امنیت در این دو حوزه را ارائه خواهیم داد.

۲. تهدیدات امنیتی در اینترنت اشیاء (IoT)

دستگاه‌های IoT به دلیل ویژگی‌های خاص خود، مانند منابع محدود، تنوع بالا و عدم وجود استانداردهای امنیتی یکپارچه، به اهداف جذابی برای مهاجمان تبدیل شده‌اند. تهدیدات امنیتی در این حوزه می‌توانند از جنبه‌های مختلفی نشأت بگیرند.

۲.۱. آسیب‌پذیری‌های دستگاه‌های IoT

- **رمزهای عبور پیش‌فرض و ضعیف:** بسیاری از دستگاه‌های IoT با رمزهای عبور پیش‌فرض و آسانی عرضه می‌شوند که کاربران اغلب آن‌ها را تغییر نمی‌دهند. این امر، دسترسی غیرمجاز به دستگاه‌ها را برای مهاجمان بسیار آسان می‌کند [2].
- **عدم به‌روزرسانی منظم نرم‌افزار:** تولیدکنندگان دستگاه‌های IoT معمولاً پشتیبانی طولانی‌مدت برای به‌روزرسانی‌های امنیتی ارائه نمی‌دهند. این موضوع باعث می‌شود که آسیب‌پذیری‌های کشف شده در نرم‌افزار دستگاه‌ها، بدون پچ باقی بمانند و مهاجمان بتوانند از آن‌ها سوءاستفاده کنند.

- **نقص‌های امنیتی در طراحی سخت‌افزار:** برخی از دستگاه‌های IoT از ابتدا با نقص‌های امنیتی در طراحی سخت‌افزاری یا نرم‌افزاری خود تولید می‌شوند که رفع آن‌ها پس از عرضه به بازار دشوار یا غیرممکن است.
- **رابط‌های کاربری ناامن:** بسیاری از دستگاه‌های IoT دارای رابط‌های کاربری وب یا موبایل هستند که ممکن است به درستی ایمن‌سازی نشده باشند و آسیب‌پذیری‌هایی مانند تزریق SQL یا XSS داشته باشند.

۲.۲. حملات رایج به IoT

- **بات‌نت‌های IoT (مانند Mirai):** یکی از خطرناک‌ترین تهدیدات، استفاده از دستگاه‌های IoT آلوده برای ایجاد **بات‌نت (Botnet)** است. بات‌نت‌ها شبکه‌هایی از دستگاه‌های آلوده هستند که توسط مهاجم کنترل می‌شوند و می‌توانند برای انجام حملات انکار سرویس توزیع شده (DDoS) در مقیاس بزرگ استفاده شوند. بدافزار Mirai در سال ۲۰۱۶ با آلوده کردن هزاران دستگاه IoT (مانند دوربین‌های مداربسته و روترها) و ایجاد یک بات‌نت عظیم، حملات DDoS بی‌سابقه‌ای را علیه وب‌سایت‌های بزرگ انجام داد [3].
- **حملات جعل هویت و دستکاری داده‌ها:** مهاجمان می‌توانند با جعل هویت دستگاه‌های IoT، داده‌های نادرست را به شبکه تزریق کنند یا داده‌های جمع‌آوری شده توسط حسگرها را دستکاری کنند. این امر می‌تواند منجر به تصمیم‌گیری‌های اشتباه در سیستم‌های خودکار شود.
- **حملات فیزیکی به دستگاه‌ها:** از آنجایی که بسیاری از دستگاه‌های IoT در محیط‌های فیزیکی قرار دارند، در معرض حملات فیزیکی مانند سرقت، دستکاری یا تخریب نیز هستند. این حملات می‌توانند منجر به از کار افتادن دستگاه یا دسترسی به اطلاعات محرمانه شوند.

۲.۳. حریم خصوصی در IoT

گسترش IoT نگرانی‌های جدی در مورد حریم خصوصی افراد ایجاد کرده است:

- **جمع‌آوری گسترده داده‌ها:** دستگاه‌های IoT به طور مداوم داده‌های مربوط به عادات، موقعیت مکانی، سلامت و سایر اطلاعات شخصی کاربران را جمع‌آوری می‌کنند. این حجم عظیم از داده‌ها می‌تواند برای پروفایل‌سازی، ردیابی و حتی سوءاستفاده‌های دیگر مورد استفاده قرار گیرد.
- **استفاده غیرمجاز از اطلاعات شخصی:** در صورت عدم وجود سیاست‌های حریم خصوصی شفاف و کنترل‌های امنیتی کافی، اطلاعات جمع‌آوری شده توسط دستگاه‌های IoT ممکن است بدون رضایت کاربر به اشتراک گذاشته یا فروخته شوند.

۳. امنیت زیرساخت‌های حیاتی

زیرساخت‌های حیاتی به سیستم‌ها و دارایی‌های فیزیکی و مجازی اطلاق می‌شود که عملکرد آن‌ها برای حفظ جامعه، اقتصاد و امنیت ملی ضروری است. هرگونه اختلال یا تخریب در این زیرساخت‌ها می‌تواند پیامدهای فاجعه‌باری داشته باشد.

۳.۱. تعریف و اهمیت زیرساخت‌های حیاتی

- **انواع زیرساخت‌های حیاتی:** شامل شبکه‌های برق، آب و فاضلاب، گاز و نفت، حمل و نقل (هوایی، ریلی، جاده‌ای، دریایی)، ارتباطات (اینترنت، تلفن)، خدمات مالی، بهداشت و درمان، و خدمات اضطراری

می‌شوند [4].

- **وابستگی متقابل و اثرات دومینو:** زیرساخت‌های حیاتی به شدت به یکدیگر وابسته هستند. به عنوان مثال، اختلال در شبکه برق می‌تواند بر سیستم‌های ارتباطی، حمل و نقل و تأمین آب تأثیر بگذارد و یک اثر دومینو ایجاد کند که منجر به فروپاشی گسترده‌تر شود.

۳.۲. تهدیدات سایبری علیه زیرساخت‌های حیاتی

با دیجیتالی شدن و اتصال زیرساخت‌های حیاتی به اینترنت، آن‌ها به اهداف جذابی برای حملات سایبری تبدیل شده‌اند. این حملات می‌توانند توسط گروه‌های تروریستی، دولت‌های متخاصم، یا حتی هکرهای مستقل انجام شوند.

- **حملات به سیستم‌های کنترل صنعتی (ICS/SCADA):** بسیاری از زیرساخت‌های حیاتی از سیستم‌های کنترل صنعتی (Industrial Control Systems - ICS) و سیستم‌های کنترل و جمع‌آوری داده (Supervisory Control and Data Acquisition - SCADA) برای نظارت و کنترل فرآیندهای فیزیکی استفاده می‌کنند. این سیستم‌ها اغلب قدیمی هستند و فاقد مکانیزم‌های امنیتی قوی می‌باشند، که آن‌ها را در برابر حملات سایبری آسیب‌پذیر می‌کند. حمله استاکس‌نت (Stuxnet) به تأسیسات هسته‌ای ایران نمونه بارزی از این نوع حملات است [5].
- **جاسوسی سایبری و خرابکاری:** مهاجمان ممکن است با هدف جاسوسی برای جمع‌آوری اطلاعات حساس در مورد عملکرد زیرساخت‌ها یا با هدف خرابکاری برای ایجاد اختلال فیزیکی، به این سیستم‌ها نفوذ کنند.
- **حملات با حمایت دولتی:** برخی از حملات پیچیده و هدفمند علیه زیرساخت‌های حیاتی توسط گروه‌های هکری با حمایت دولت‌ها انجام می‌شوند که دارای منابع و توانایی‌های بالایی هستند.

۳.۳. پیامدهای حملات به زیرساخت‌های حیاتی

- **اختلال در خدمات عمومی:** حملات موفق می‌توانند منجر به قطع برق، آب، گاز، اختلال در حمل و نقل عمومی و از کار افتادن سیستم‌های ارتباطی شوند که زندگی روزمره میلیون‌ها نفر را تحت تأثیر قرار می‌دهد.
- **خسارات اقتصادی و جانی:** اختلال در زیرساخت‌ها می‌تواند منجر به خسارات اقتصادی میلیاردها دلاری شود. در موارد شدیدتر، مانند حملات به سیستم‌های بهداشتی یا حمل و نقل، ممکن است تلفات جانی نیز به همراه داشته باشد.

۴. راهکارهای افزایش امنیت IoT و زیرساخت‌های حیاتی

تقویت امنیت در حوزه‌های IoT و زیرساخت‌های حیاتی نیازمند یک رویکرد جامع، چندوجهی و همکاری بین‌المللی است.

۴.۱. استانداردهای امنیتی و مقررات

- **توسعه و اجرای استانداردهای امنیتی برای دستگاه‌های IoT:** دولت‌ها و سازمان‌های استاندارد باید استانداردهای امنیتی سختگیرانه‌ای را برای تولیدکنندگان دستگاه‌های IoT وضع کنند. این استانداردها باید

شامل الزاماتی مانند رمزهای عبور پیش‌فرض قوی، قابلیت به‌روزرسانی امن نرم‌افزار، و مکانیزم‌های امنیتی داخلی باشند [6].

- **قوانین و سیاست‌های حفاظت از زیرساخت‌های حیاتی:** کشورها باید قوانین و مقرراتی را برای الزام اپراتورهای زیرساخت‌های حیاتی به رعایت استانداردهای امنیتی سایبری و گزارش حوادث امنیتی تدوین کنند. نهادهایی مانند CISA در ایالات متحده نقش مهمی در این زمینه ایفا می‌کنند.

۴.۲. معماری امنیتی قوی

- **جداسازی شبکه (Network Segmentation):** برای کاهش دامنه حملات، شبکه‌های IoT و ICS/SCADA باید از شبکه‌های IT سازمانی جدا شوند. این جداسازی باعث می‌شود که در صورت نفوذ به یک بخش از شبکه، مهاجم نتواند به راحتی به بخش‌های حیاتی دیگر دسترسی پیدا کند.
- **احراز هویت قوی و مدیریت دسترسی:** استفاده از احراز هویت چندعاملی (MFA) برای دسترسی به دستگاه‌های IoT و سیستم‌های کنترل صنعتی ضروری است. همچنین، باید اصل کمترین امتیاز (Least Privilege) در مدیریت دسترسی‌ها رعایت شود، به این معنی که هر کاربر یا دستگاه فقط به حداقل دسترسی‌های لازم برای انجام وظایف خود نیاز داشته باشد.
- **رمزنگاری داده‌ها در حال انتقال و ذخیره‌سازی:** تمام داده‌های حساس در دستگاه‌های IoT و زیرساخت‌های حیاتی باید در حالت انتقال و ذخیره‌سازی رمزنگاری شوند تا از دسترسی غیرمجاز محافظت شوند.

۴.۳. نظارت و تشخیص تهدید

- **سیستم‌های تشخیص نفوذ (IDS) و مدیریت رویدادهای امنیتی (SIEM):** استقرار IDS/IPS برای شناسایی فعالیت‌های مشکوک و SIEM برای جمع‌آوری، تحلیل و همبسته‌سازی لاگ‌های امنیتی از سراسر شبکه، برای تشخیص زودهنگام حملات حیاتی است.
- **تحلیل رفتاری و هوش مصنوعی در امنیت:** استفاده از هوش مصنوعی و یادگیری ماشین برای تحلیل الگوهای رفتاری عادی در شبکه‌های IoT و ICS/SCADA می‌تواند به شناسایی ناهنجاری‌ها و تهدیدات ناشناخته کمک کند.

۴.۴. همکاری بین‌المللی و اشتراک اطلاعات

- **همکاری بین‌المللی:** تهدیدات سایبری مرز نمی‌شناسند. همکاری بین‌المللی بین دولت‌ها، سازمان‌های امنیتی و بخش خصوصی برای اشتراک‌گذاری اطلاعات تهدید، توسعه استانداردهای مشترک و هماهنگی پاسخ به حملات ضروری است.
- **اشتراک اطلاعات تهدید:** ایجاد پلتفرم‌هایی برای اشتراک‌گذاری اطلاعات در مورد تهدیدات سایبری، آسیب‌پذیری‌ها و بهترین شیوه‌های امنیتی بین ذینفعان مختلف (مانند ISACs - Information Sharing and Analysis Centers) می‌تواند به بهبود وضعیت امنیتی کلی کمک کند [7].

۵. نتیجه‌گیری

اینترنت اشیاء و زیرساخت‌های حیاتی، دو ستون اصلی جامعه دیجیتالی مدرن را تشکیل می‌دهند. در حالی که این فناوری‌ها مزایای بی‌شماری را به ارمغان می‌آورند، آسیب‌پذیری‌های ذاتی و وابستگی متقابل آن‌ها، چالش‌های امنیتی بی‌سابقه‌ای را نیز ایجاد کرده است. از بات‌نت‌های IoT که حملات DDoS را در مقیاس جهانی انجام می‌دهند تا حملات هدفمند علیه سیستم‌های کنترل صنعتی که می‌توانند منجر به اختلال در خدمات حیاتی شوند، پیامدهای نقص امنیتی در این حوزه‌ها می‌تواند فاجعه‌بار باشد.

مقابله با این تهدیدات نیازمند یک رویکرد جامع و چندوجهی است که شامل توسعه و اجرای استانداردهای امنیتی قوی، طراحی معماری‌های امنیتی مقاوم، نظارت مستمر و تشخیص پیشرفته تهدیدات، و همکاری گسترده در سطح ملی و بین‌المللی باشد. تولیدکنندگان دستگاه‌های IoT باید امنیت را از مرحله طراحی در نظر بگیرند، اپراتورهای زیرساخت‌های حیاتی باید سرمایه‌گذاری کافی در امنیت سایبری انجام دهند، و دولت‌ها باید چارچوب‌های قانونی و نظارتی مناسب را فراهم کنند. با اتخاذ این رویکرد جامع، می‌توانیم از پتانسیل کامل اینترنت اشیاء بهره‌مند شویم و در عین حال، از زیرساخت‌های حیاتی خود در برابر تهدیدات سایبری محافظت کنیم و آینده‌ای امن‌تر و پایدارتر را تضمین نماییم.

۶. منابع

[1] ITU-T. (2012). *Recommendation Y.2060: Overview of the Internet of Things*. Available at: https://www.itu.int/rec/T-REC-Y.2060-201206-I/en [2] OWASP Foundation. (Ongoing). *OWASP IoT Top 10*. Available at: https://owasp.org/www-project-iot-top-10/ [3] KrebsOnSecurity. (2016). *Who Makes the IoT Things Hacking Your Site?*. Available at: https://krebsonsecurity.com/2016/10/who-makes-the-iot-things-hacking-your-site/ [4] Cybersecurity & Infrastructure Security Agency (CISA). (Ongoing). *Critical Infrastructure Sectors*. Available at: https://www.cisa.gov/critical-infrastructure-sectors [5] Langner, R. (2011). *Stuxnet: Dissecting a Cyberwarfare Weapon*. IEEE Security & Privacy, 9(3), 49-51. Available at: https://ieeexplore.ieee.org/document/5775793 [6] NIST. (2020). *NIST Special Publication 800-213: IoT Device Cybersecurity Guidance for the Federal Government*. Available at: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-213.pdf [7] National Council of ISACs. (Ongoing). *About ISACs*. Available at: https://www.nationalisacs.org/about-isacs/ [8] European Union Agency for Cybersecurity (ENISA). (2020). *Baseline Security Requirements for IoT in the context of Critical Information Infrastructures*. Available at: https://www.enisa.europa.eu/publications/baseline-security-requirements-for-iot-in-the-context-of-critical-information-infrastructures [9] World Economic Forum. (2020). *The Global Risks Report 2020*. Available at: https://www.weforum.org/reports/the-global-risks-report-2020/ [10] International Electrotechnical Commission (IEC). (Ongoing). *IEC 62443: Security for industrial automation and control systems*. Available at: https://www.iec.ch/homepage (Search for IEC 62443)