APJ. 4(1):8-17, Spring 2023

Arman Process Journal (APJ)

Homepage: armanprocessjournal.ir

Cyber Security in the Field of Internet of Things

M. Hoseinzadeh[*,1] **, A. Rezaei**[*,2]

[1] Computer Engineering Department, Islamic Azad University (IAU), Science and Research Branch, Tehran, Iran
[2] Computer Engineering Department, Islamic Azad University (IAU), Science and Research Branch, Tehran, Iran

ABSTRACT

The Internet of Things is a novel and popular technology in which the ability to send data through communication networks, either the Internet or intranet, is provided. Connecting more devices to the Internet will lead to security threats, and providing security in the Internet of Things is recognized as a necessity and can be considered as one of the most important challenges of the Internet of Things. Cyber security has always been one of the concerns of the Internet of Things field. Cyber security of the Internet of Things is a specific part of the technology field that focuses on the protection of devices and networks connected to the Internet of Things and includes various equipment, including mechanical machines and He mentioned digital, computing devices, technologies such as artificial intelligence, etc. Also, security breaches and privacy violations are some of the major challenges in this field that sometimes prevent the widespread use of the Internet of Things. Therefore, according to the necessity of research in this article, we will examine some related attacks and solutions in the field of Internet of Things cyber security.

Received: 8 Match 2023
Accepted: 10 June 2023

KEYWORDS:
Cybersecurity,
Internet of Things
Confidentiality,
Access Control,
Validation,

[1] Corresponding author
ma.hoseinzadeh@srbiau.ac.ir

NUMBER OF REFERENCES	NUMBER OF FIGURES	NUMBER OF TABLES
19	0	0

فصلنامه تخصصی آرمان پردازش
(APJ)
Homepage: www.armanprocessjournal.ir

امنیت سایبری در حوزه اینترنت اشیاء

مرضیه حسین زاده*[۱]، علیرضا رضائی*[۲]

[۱] دانشکده مهندسی کامپیوتر، دانشگاه آزاد اسلامی، واحد علوم و تحقیقات، تهران، ایران
[۲] دانشکده مهندسی کامپیوتر، دانشگاه آزاد اسلامی، واحد علوم و تحقیقات، تهران، ایران

چکیده

اینترنت اشیا فناوری جدید و محبوبی است که در آن قابلیت ارسال داده از طریق شبکه های ارتباطی، اعم از اینترنت یا اینترانت، فراهم میگردد. اتصال دستگاه های بیشتر به اینترنت تهدیدات امنیتی را به دنبال خواهد داشت و تامین امنیت در اینترنت اشیاء یک ضرورت شناخته می شود و می توان آز آن به عنوان یکی از مهمترین چالش های اینترنت اشیاء یاد کرد. امنیت سایبری همواره یکی از دغدغه های حوزه اینترنت اشیاء بوده است. امنیت سایبری اینترنت اشیا بخش مشخصی از حوزه تکنولوژی است که بر حفاظت از دستگاهها و شبکههای متصل به اینترنت اشیا تمرکز دارد و شامل تجهیزات مختلفی است که از جمله آنها میتوان به ماشینهای مکانیکی و دیجیتال، دستگاههای محاسباتی، تکنولوژیهایی مانند هوش مصنوعی و ... اشاره کرد. همچنین رخنه های امنیتی و نقض حریم خصوصی، برخی از چالش ها مسائل عمده ای در این حوزه هستند که گاها از کاربرد گسترده ی اینترنت اشیاء جلوگیری می کنند. لذا با توجه به ضرورت تحقیق در این مقاله، به بررسی برخی از حملات و راهکارهای مرتبط در حوزه امنیت سایبری اینترنت اشیاء می پردازیم.

واژگان کلیدی:
امنیت سایبری،
اینترنت اشیاء،
محرمانگی،
کنترل دسترسی،
تایید اعتبار،

تعداد جداول	تعداد شکل ها	تعداد مراجع
۰	۰	۱۹

مقدمه

امروزه دستاوردهای حوزه فناوری‌های اطلاعات و ارتباط از جمله خدمات مبتنی بر اینترنت اشیاء[1] تبدیل به عنصر حیاتی زندگی علاقه مندان و کاربران خبره این تکنولوژی ها گشته است و این دستاوردها با سرعت روزافزون روز به روز در حال گسترش و پیشرفت می باشند. اینترنت اشیاء یعنی ارتباط حسگرها و دستگاه‌ها با شبکه اینترنت که از طریق این ارتباط و تعامل بین لوازم متصل به شبکه و کاربران دارای دسترسی مجاز به این شبکه، امکان دیدن و کنترل لوازم متصل به شبکه برای کاربران آن فراهم می‌شود. این مفهوم می‌تواند به سادگی ارتباط یک گوشی هوشمند با تلویزیون یا به پیچیدگی نظارت بر زیرساخت‌های شهری و ترافیک باشد. این شبکه طیف بسیاری از دستگاه‌های اطراف ما را دربرمی‌گیرد. اینترنت اشیاء دارای پتانسیل های بسیاری در زمینه های صنعت و سبک زندگی و کسب و کار انسان ها دارد. این فناوری می تواند توانایی انسان در پردازش و انتقال داده ها و اطلاعات چندین برابر کند. در دنیای جدیدی که اینترنت اشیاء در آن حضور دارد دسترسی بیشتر به اطلاعات به مفهوم کنترل بهتر آینده است. در اینترنت اشیاء بدون نیاز ارتباط انسان با انسان و یا انسان با کامپیوتر اطلاعات ارسال می شوند. گفته می شود در دنیایی که بر اینترنت اشیاء مبتنی باشد عدم دسترسی به داده ها بی معنی خواهد بود و این بدین معنی است که کارایی نیروهای کار افزایش پیدا خواهد کرد [۲-۱].

همسو با این پیشرفت های فناوری در حوزه اینترنت اشیاء نیازهای کاربران خدمات این حوزه مانند حفاظت از کارائی، پردازش سریع، دسترسی پویا به منابع زیرساختی، ایجاد مشارکت متقابل با کمترین هزینه، نیز اهمیت زیادی یافته اند. دسترسی داشتن به اطلاعات بیشتر منجر به تولید محصولاتی خواهد شد که سهولت بیشتری را به زندگی انسان ها به ارمغان خواهد آورد، اما تسهیل زندگی بشر امروزی پیچیدگی های دنیای مدرن را به دنبال خواهد داشت. اینترنت اشیاء نیز در مسیر این تسهیل ایجاد شده است و انتقال اطلاعات موجب سهولت در زندگی بشر و در عین حال پیچیدگی خواهد شد. از طرفی ارتباط موثرتر تولید کنندگان و مصرف کنندگان موجب خدمات رسانی بهتر و همچنین کاهش هزینه های زنجیره تولید و عرضه کالا خواهد شد. رشد و توسعه دنیای دیجیتالی که امروز در آن زندگی می‌کنیم در کنار تمام ویژگی‌های مثبتی که دارد چالش‌ها و مسایلی را هم به وجود آورده است . باید این مهم را مدنظر داشت که اتصال دستگاه های بیشتر به اینترنت تهدیدات امنیتی را به دنبال خواهد داشت و تامین امنیت در اینترنت اشیاء یک ضرورت شناخته می شود و می توان آز آن به عنوان یکی از مهمترین چالش های اینترنت اشیاء یاد کرد. امنیت در اینترنت اشیاء یکی از مهم‌ترین موضوعاتی است که باید مورد توجه قرار گیرد. با توجه به اینکه تعداد دستگاه‌های متصل به اینترنت اشیاء هر روز در حال افزایش است، حفظ امنیت این دستگاه‌ها و اطلاعاتی که به آن‌ها دسترسی دارند، بسیار حائز اهمیت است.

از آنجائی که اینترنت اشیاء در صنایع مختلف مورد استفاده قرار می‌گیرد به طور مثال خودرو و ناوگان حمل و نقل، هوانوردی، کشاورزی، واحدهای تبریدی و ... ، لذا کسب و کارها و ارگان‌ها بایستی بیشتر به امنیت اینترنت اشیاء اهمیت دهند. چرا که کوچک‌ترین اختلال می‌تواند عواقب جبران ناپذیری را به بار بیاورد [۳] . درحال حاضر بیش از ۹ میلیارد شی به اینترنت متصل هستند و این می‌تواند زنگ خطری باشد؛ به این معنا که امنیت در اینترنت اشیاء از صحبت‌های میان کارشناسان و نظریه‌های معرفی‌شده، تبدیل به چالش اصلی در بحث تهدیدات امنیت شبکه شده است. براساس گزارش های اخیر از شرکت‌کنندگان در نظرسنجی گسترش اینترنت اشیاء، بسیاری بر این باورند که چالش تکنولوژی‌محور بودن پیاده‌سازی اینترنت اشیاء، چالش شماره یک امنیت سایبری محسوب می‌شود. آنچه اهمیت دارد این است که محافظت از موجودیت‌هایی که دیده نمی‌شود، بسیار مشکل و غیرممکن است. چگونه می‌توانید از تجهیزاتی که به شبکه شما متصل است اما شما هیچ‌گونه شناخت و اطلاعاتی از آن‌ها ندارید، محافظت کنید؟ این یکی از سوال‌های مناسب است که می‌تواند اهمیت شفافیت در شبکه‌های تجاری و سازمانی را از نظر امنیت مشخص کند. این در حالی است که در آینده نه چندان دور، تجهیزات اینترنت اشیاء نیز به شبکه‌های تجاری و سازمانی متصل خواهند شد؛ هر چند که تاکنون نیز امکان دارد در بسیاری از این شبکه‌ها تجهیزات اینترنت اشیاء وجود داشته باشند. به عنوان مثال می‌توان به تجهیزات پزشکی و آزمایشگاهی اشاره کرد. در بسیاری از داشبوردهای مانیتورینگ شبکه‌های تجاری در حدود ۴۰ تا ۶۰ درصد از تجهیزات متصل، در وضعیت ناشناس قرار دارند و هرچه مقیاس شبکه بزرگ‌تر می‌شود، این اعداد نیز بزرگتر می‌شوند. بیشتر تجهیزاتی که در این وضعیت قرار ندارند مواردی غیر از کامپیوتر، پرینتر یا تبلت‌ها هستند که این تجهیزات می‌توانند مواردی مانند دوربین‌های امنیتی، تجهیزات پزشکی و... باشند. پروفایل‌سازی این تجهیزات به صورت دستی، کار بسیار فرسایشی و با هزینه زیاد و همچنین بی‌فایده مخصوصا در مقیاس‌های بزرگ برای سازمان است. حالا فرض کنید که این امکان به وجود بیاید که امکان شناسایی این تجهیزات به صورت خودکار به وجود آید، چه تغییراتی در بحث شفافیت ایجاد خواهد شد. لذا مساله امنیت و مسائل مرتبط با آن از ابعاد مهم مدیریتی در حوزه کاربردهای اینترنت اشیاء می باشد [۴].

در این حوزه، امنیت سایبری بر محافظت از ماشین های کامپیوتری که دارای سیستم عامل هستند، و الکترونیکی که قابل برنامه ریزی می باشند، در برابر دسترسی غیرمجاز یا آسیب دیدگی یا غیرقابل دسترس شدن تاکید دارد. امنیت اطلاعات مقوله وسیع تری است که از تمامی دارایی های اطلاعاتی چه به صورت چاپی و چه دیجیتال محافظت می

[1] Internet of Things (IoT)

کند. با توجه به اهمیت موضوع، در این مقاله قصد داریم به جنبه های عمومی بحث امنیت سایبری در حوزه اینترنت اشیاء بپردازیم.

امنیت سایبری در اینترنت اشیاء و حملات مرتبط

اینترنت اشیاء، دستگاه‌های مختلف را از طریق اینترنت به هم متصل می‌کند تا با دستگاه‌های دیگری که به همان شبکه متصل شده‌اند، ارتباط برقرار کنند. گسترش و پیشرفت در قابلیت‌های شبکه، باعث بهبود در روند زندگی، صرفه‌جویی در زمان و هزینه می‌شود. از سوی دیگر بهره گیری از این خدمات چالش های امنیتی به دنبال دارد. در واقع، امنیت در اینترنت اشیاء اصلی ترین چالش پیش روی اینترنت اشیاء برای گسترش در بین جوامع محسوب می گردد . تأکید عمده این مقاله بر موضوعات امنیت سایبری حاکم با گسترش اینترنت اشیاء است. اساسا حمله سایبری تلاش مجرمان برای غیرفعال کردن رایانه‌ها، سرقت داده‌ها یا استفاده از یک سیستم رایانه‌ای نقض شده برای انجام حملات اضافی است. حملات سایبری در سال‌های اخیر پیچیده‌تر شده‌اند و در نتیجه، پیشگیری از حملات سایبری برای هر فرد و سازمانی ضروری است. جرایم سایبری مبتنی بر بهره برداری مؤثر از آسیب پذیری ها است. همانطور که کارشناسان امنیت به طور مداوم تاکید دارند، افزایش سطح حمله، امکان حمله‌ی مجرمان سایبری را افزایش می‌دهد. به همین دلیل، متخصصان امنیت سایبری سعی می‌کنند خطرات و مشکلات امنیتی در این حوزه را مدیریت کنند . امنیت سایبری اینترنت اشیاء، بخشی از فناوری است که به حفاظت از دستگاه‌ها و شبکه‌های متصل در اینترنت اشیاء می‌پردازد. در اینترنت اشیاء، به هر شیء یک شناسه منحصر به‌فرد اختصاص داده می‌شود و به صورت خودکار می‌توانند داده‌ها را در سراسر شبکه، انتقال دهند. در این حوزه، اگر امنیت مد نظر قرار نگیرد، امکان اتصال دستگاه‌ها به اینترنت، آن‌ها را در معرض چندین خطر عمده قرار می‌دهد. بصورت بنیادین، انواع مختلفی از حمله های رایج در حوزه اینترنت اشیاء وجود دارند که در ادامه به بررسی آن‌ها خواهیم پرداخت [۶-۵].

استراق سمع

اتصالات ضعیف و حفره‌های امنیتی به مهاجمان این امکان را می‌دهند که تماس‌های صوتی و تصویری را کنترل کنند. حتی سارقان با تکنیک‌های امروزی خود قادرند که از طریق یک لامپ آویزان هم مکالمات جاری در یک اتاق را ضبط نمایند.

ترفیع امتیاز

در این حملات مهاجمان از باگ‌ها و پیکربندی‌های نادرست سیستم‌ها سو استفاده می‌کنند و از این طریق به شکل غیر مجاز به امتیازاتی دست می‌یابند و درحالت دسترسی ممتاز و غیرمجاز فعالیت می نمایند.

جستجوی فراگیر

همیشه به کاربران توصیه می‌شود که برای دستگاه‌ها و سیستم‌های خود رمزهای پیچیده و دشواری انتخاب کنند. چرا که مهاجمان در جستجوی فراگیر با بررسی رمزهای رایج و آسان به سرعت سیستم شما را هک می‌نمایند. احراز هویت چند مرحله‌ای و روش اعتماد صفر، خطر این حملات را کاهش می‌دهند [۷].

حملات مبتنی برMAC

MAC رابطی است که انتقال داده‌ها را در دستگاه‌های اینترنت اشیاء آسان می‌کند و همچنین اجازه می‌دهد که چندین کاربر از یک محیط فیزیکی بهره ببرند. مهاجمان می‌توانند با جعل MAC به سیستم‌ها نفوذ نمایند. یکی از نگرانی های کلیدی مربوط به پذیرش موفقیت آمیز اینترنت اشیاء، داشتن مکانیزم های امنیتی کاملا قوی در سراسر اکوسیستم است تا بتواند خطرات امنیتی افزایش یافته در اتصال دستگاه ها به اینترنت را کاهش دهد. همان طور که گسترش دنیای اینترنت اشیاء مزایای بیشماری را به همراه خود می آورد، در مقابل به میزان مخاطرات احتمالی همراه با آن نیز افزوده می شود. چرا که مجرمان و هکرها می توانند از هر یک از دستگاه های جدید به عنوان یک دروازه ی نو به دنیای هک و حملات سایبری استفاده کنند. مجرمان سایبری انگیزه می گیرند تا روش های جدید و حیرت انگیزی را برای هک کردن دستگاه های بی خطر بدست آورند تا به وسیله ی آن ها به دستگاه های با ارزش تر راه یابند [۹-۸].

دستگاه‌ها

دستگاه‌ها می‌توانند ابزار اصلی برای پیشبرد حملات سایبری باشند. حافظه، میان افزار، رابط فیزیکی، رابط وب و زیرساخت شبکه، همه حوزه‌هایی هستند که احتمال وقوع آسیب‌پذیری در آن زیاد است. حمله‌کنندگان همچنین می‌توانند از تنظیمات پیش‌فرض ناامن، اجزای قدیمی و منسوخ شده، و مکانیسم‌های به‌روزرسانی غیر ایمن و سایر عوامل استفاده کنند.

کانال‌های ارتباطی در اینترنت اشیاء

حمله به دستگاه‌های اینترنت اشیاء می‌تواند از طریق کانال‌های ارتباطی که واسط ها و اجزای اینترنت اشیاء را به یکدیگر متصل می‌کنند، آغاز شود. پروتکل‌های استفاده شده در سیستم‌های اینترنت اشیاء ممکن است دارای نقاط ضعف امنیتی باشند که روی کل سیستم تاثیر خواهد داشت. علاوه بر این‌ها، سیستم‌های آن می‌تواند در معرض حملات شبکه‌ای معروف مانند حملات منع سرویس (DoS) و تقلید (Spoofing) قرار بگیرند [۱۱-۱۰].

نرم‌افزارها و اپلیکیشن‌ها

آسیب‌پذیری‌های موجود در برنامه‌های وب و نرم‌افزارهای مرتبط با دستگاه‌های اینترنت اشیاء می‌تواند سلامت امنیتی سیستم‌های مرتبط را به خطر بیاندازد. به عنوان مثال، برنامه‌های وب ممکن است برای دزدیدن اطلاعات اعتبارنامه کاربران یا توزیع به‌روزرسانی نرم‌افزاری مخرب استفاده شوند. به عنوان نمونه استاکس‌نت (Stuxnet) یک کرم کامپیوتری پیچیده است که برای تشخیص ماشین‌آلات هسته‌ای خاص طراحی شده است. استاکس‌نت به جای هک کردن دستگاه‌ها برای ایجاد خسارت نرم‌افزاری، آن‌ها را نابود می‌کند. همچنین Mirai اینترنت را برای یافتن دستگاه‌های اینترنت اشیاء که از پردازنده ARC استفاده می‌کنند، جستجو می‌کند. پردازنده ARC یک نسخه ساده شده از سیستم عامل لینوکس را اجرا می‌کند. اگر نام کاربری و رمزعبور پیش‌فرض دستگاه تغییر نکند، Mirai می‌تواند دستگاه را آلوده کرده و آن را تحت کنترل خود درآورد [۱۳-۱۲].

راهکارهای امنیت سایبری در اینترنت اشیا

برای حفاظت از دستگاه‌ها و شبکه‌های مبتنی بر اینترنت اشیاء در برابر حملات سایبری، می‌توان اقدامات زیر را در نظر گرفت:

انتخاب رمز عبور قوی و تغییر رمز پیش فرض

قبل از اتصال به شبکه، دستگاه‌های متصل به اینترنت اشیاء باید ایمن شوند. برای انجام این کار، از رمزهای عبور قوی استفاده کنید، نرم‌افزار امنیتی این دستگاه‌ها را به‌روز نگه دارید و دستگاه را رمزگذاری و احراز هویت کنید. همچنین بسیاری از دستگاه‌های اینترنت اشیاء دارای رمز عبورهای پیش‌فرض هستند که مجرمان سایبری آن‌ها را می‌دانند. بدین ترتیب، حتما بایستی رمزعبور پیش فرض خود را تغییر دهید تا از دسترسی غیرمجاز به دستگاه‌های اینترنت اشیاء خود جلوگیری کنید.

ایجاد شبکه‌های مهمان

ایمن‌سازی اتصالات شبکه و Wi-Fi با رمزهای عبور قوی بسیار مهم است. همچنین ایجاد شبکه‌های مهمان[1] برای جلوگیری از دسترسی هکرها به اتصال و اطمینان از امنیت دستگاه‌های اینترنت اشیاء ضروری است.

بررسی تنظیمات پیش فرض

بسیاری از دستگاه‌های اینترنت اشیاء شامل تنظیمات پیش‌فرض امنیت و حریم خصوصی هستند. برای جلوگیری از حملات سایبری، می‌توانید این تنظیمات را بررسی و تغییر دهید. برخی از تنظیمات پیش‌فرض ممکن است مزیتی برای تولیدکننده دستگاه داشته باشند.

به‌روزرسانی مداوم دستگاه

به روزرسانی نرم‌افزار دستگاه‌های اینترنت اشیاء بسیار حائز اهمیت است. با به روزرسانی نرم‌افزار، مشکلات امنیتی رفع می‌شود و دستگاه‌ها در برابر حملات جدید مقاومت بیشتری خواهند داشت .بنابراین، هر دستگاه باید دارای قابلیت به روزرسانی نرم‌افزار باشد. درست مانند به‌روزرسانی‌های تلفن همراه، سازندگان دستگاه‌های اینترنت اشیاء، ممکن است به‌روزرسانی‌هایی را برای نرم‌افزار امنیتی جدید ارسال کنند. همچنین می‌توانید وب‌سایت‌های آن‌ها را برای به‌روزرسانی و محافظت از اینترنت اشیاء بررسی کنید. بهترین برنامه‌های صدور گواهینامه امنیت سایبری حادث را بررسی کنید تا در مورد گواهینامه‌هایی که برای شروع یا پیشرفت حرفه امنیت اطلاعات خود باید دنبال کنید، آشنا شوید.

بهره گیری از بلاکچین

در ایجاد یک استراتژی امنیت سایبری برای اینترنت اشیاء بهتر است فناوری بلاکچین را به عنوان یک رویکرد اصلی در نظر بگیرید. بلاکچین دارای یک فضای ذخیره‌سازی غیر متمرکز است که اطلاعات را به صورت دیجیتالی در قالبی شفاف و قابل دسترسی نگهداری می‌کند. بلاکچین یک سیستم غیرمتمرکز است که بسیاری از شبکه‌ها و گره‌ها را در بر می‌گیرد. هر گره در واقع یک دستگاه الکترونیکی است که یک نسخه از زنجیره بلاک را حفظ می‌کند، در نتیجه حمله به یک یا چند گره تأثیری بر سایر گره‌های دیگر نخواهد داشت. به طور پیش‌فرض، فناوری بلاکچین با محدود کردن دسترسی به اپلیکیشن ها و دستگاه‌های اینترنت اشیاء، از تغییرات غیرمجاز در داده‌ها جلوگیری می‌کند و امکان غیرفعال و خاموش کردن دستگاه‌های در معرض خطر در اکوسیستم شبکه را فراهم می‌کند [۱۴].

ارزیابی های منظم دوره ای

در هنگام ارزیابی، انتخاب و نصب دستگاه‌های اینترنت اشیاء، امنیت سایبری از ابتدا باید در اولویت قرار گیرد و بصورت منظم ارزیابی های دوره ای امنیتی و محافظتی صورت پذیرد. امنیت دستگاه هرگز نباید بعد از اتمام فرآیند اضافه شود. به روزرسانی‌های نرم‌افزاری، خطرات سایبری را کاهش می‌دهند. در نظر داشته باشید که فقط روی دستگاه‌هایی سرمایه‌گذاری کنید که قادر به اجرای نرم‌افزار و به روزرسانی‌های نرم‌افزاری در بازه‌های منظم ارزیابی را داشته باشند.

تحلیل پیشگیرانه

آنالیز، به دستگاه‌ها و سیستم‌های هوشمند این قابلیت را می‌دهد تا به مرور زمان الگوی استفاده‌ی کاربر خود را شناسایی و ذخیره‌سازی نمایند. در نتیجه هرگونه تغییری شناسایی و نسبت به آن واکنش نشان داده می‌شود. برای امنیت دستگاه‌های اینترنت اشیاء به صورت پیشگیرانه

[1] Guest Networks

شرایط را تحلیل و عمل کنید. نرم‌افزارهای رایگان به ندرت به صورت رسمی در ابر، لبه شبکه یا در دستگاه نگهداری می‌شوند. هزینه تلاش برای بازیابی پس از یک حمله سایبری بسیار بیشتر از ایمن‌سازی دستگاه اینترنت اشیاء و شبکه در ابتدا است. از متخصصان کمک بخواهید. امنیت سایبری یک هدف متعالی است که همواره در حال تغییر است و به نظر می‌رسد که هکرها همیشه یک قدم جلوتر هستند. به همین دلیل، امنیت سایبری تبدیل به مهارتی شده است که بسیاری از سازمان‌ها در آن کمبود و ضعف تکنولوژیکی دارند. اعمال امنیت سایبری هوشمندانه امری دشوار است و برای بهره‌برداری کامل از آن‌ها، نیاز به تعهد مداوم و پیوسته وجود دارد. بنابراین، یک رویکرد تحلیل محور پیشگیرانه و سیستمی به امنیت سایبری به طور کامل نتایج خوبی در کوتاه مدت و بلند مدت به همراه خواهد داشت [۱۶-۱۵].

شناسایی دستگاهها و صدور گواهینامه های دیجیتال

این کار برای محدود کردن دسترسی به دستگاه متصل و داده‌هایی که تولید می‌کند، به افراد و برنامه‌های مجاز استفاده می‌شود. گواهینامه های دیجیتال نیز به یک موجودیت دیجیتالی مانند دستگاه اینترنت اشیاء، کامپیوتر و... امکان انتقال اطلاعات به طرف‌های مجاز را به صورت امن می‌دهند. گواهی‌نامه‌های X509 فرمت‌های معمولی گواهی هستند که به طور معمول توسط یک مرجع معتبر گواهی‌دهنده امضا می‌شوند. آن‌ها به ما امکان می‌دهند هر دستگاه اینترنت اشیاء را به طور منحصر به فرد شناسایی و تأیید کنیم.

احراز هویت و اعتبارسنجی

علاوه بر موارد ذکر شده، برای کاهش خطر نفوذ در یک شرکت، باید در رویه‌های سختگیرانه‌ی احراز هویت و اعتبارسنجی دستگاه تمرکز کرد، که قادر به حفاظت از رابط‌های موبایل و ابری باشد. کسب‌وکارها باید اطمینان حاصل کنند که هر دستگاه اینترنت اشیاء متصل به شبکه خود، دارای یک گواهی استاندارد X.509 است. با استفاده از این گواهی، مدیر OTمی‌تواند هر دستگاه اینترنت اشیاء را شناسایی و اعتبارسنجی کند. در صورتی که مورد مشکوکی پیدا شود، می‌توان دستگاه را از شبکه جدا کرد. این امر به‌طور چشمگیری مشکلات امنیتی اینترنت اشیاء را کاهش می‌دهد .همچنین فناوری‌های هویت عملی مانند اثر انگشت، شناسایی چهره و کارت‌های هوشمند، می‌تواند در تشخیص افراد خرابکار یا قابل اعتماد کمک کنند.

احراز هویت دو عامله[1]

برخی از سازمان ها برای احراز هویت ، از احراز دو عامله (2FA) استفاده می کنند. در این روش نیاز است که کاربر یک رمز عبور را وارد کند، همچنین از یک فاکتور تصدیق مجدد مانند یک کد تصادفی که از طریق پیام متنی (SMS) ایجاد شده است برای تایید رمز عبور و در نتیجه احراز هویت استفاده می شود. برای برنامه های اینترنت اشیاء، استفاده از این روش احراز هویت، احراز هویت متنی یا تایید هویت سازگار ایده ی بسیار خوبی است. این روش ها شامل استفاده از اطلاعات متنی و الگوریتم های یادگیری ماشین هستند که دائما خطرات ممکن را بررسی می کنند؛ بدون آنکه روی تجربه کاربر در استفاده از برنامه ها و محصولات اینترنت اشیاء اثر بگذارد.

رمزنگاری

استفاده از رمزنگاری های قوی برای حفاظت از پروتکل ها، یکی دیگر از شیوه های امنیتی خوب در شبکه است. رمزنگاری ابزاری قدرتمند برای مقابله با مسائل امنیتی داده‌ها است. برای تضمین محرمانگی و حریم خصوصی، شرکت‌ها باید از رمزگذاری قوی برای داده‌های خود استفاده کنند. این امر در هنگام وقوع نقض امنیتی یا حمله سایبری بسیار مفید است. اینترنت اشیاء در لایه های مختلف بسیاری از پروتکل های شبکه را شامل می شوند؛ پس امکان هک کردن هر گونه ارتباطی بین دستگاه ها وجود دارد. رمز کردن لایه های Network و Transport می تواند موانع متعددی در برابر حملات تحت شبکه ایجاد کند.

ایمن سازی واسط های دسترسی

یکی از روش های مناسب برای افزایش امنیت، استقرار یک رویکرد لایه ای واسط است، به این ترتیب مهاجمان باید موانع متعددی را که برای محافظت از دستگاه ها و جلوگیری از ورود اطلاعات و دسترسی های غیر مجاز طراحی شده اند ، دور بزنند .شرکت ها باید از آسیب پذیری های شناخته شده نظیر پورت های بازTCP / UDP ، پورت های سریال باز، درخواست رمز عبور باز ، مکان هایی برای تزریق کد از جمله سرور های وب ، ارتباطات بدون رمزگذاری و اتصالات رادیویی محافظت کنند. یکی دیگر از اقدامات خوب برای محافظت سایبری در این حوزه، ارتقاء واسط های دسترسی به دستگاهها با نصب پچ های امنیتی مورد نیاز است. اما به یاد داشته باشید که بسیاری از فروشندگان دستگاه در هنگام ساخت و فروش دستگاهها بر امنیت تمرکز نمی کنند. طبق مطالعات انجام شده ، بسیاری از دستگاه های اینترنت اشیاء unpatchable هستند و به همین علت از امنیت لازم برخوردار نیستند. پس قبل از سرمایه گذاری در دستگاه هایی که از طریق اینترنت اشیاء متصل می شوند، قابلیت های امنیتی دستگاه ها را ارزیابی کنید و مطمئن شوید که توسعه دهندگان از ابزارهای کافی برای ارزیابی عملکرد امنیتی دستگاه های خود برخوردارند. یکی دیگر از مسایل مهمی که باید مورد توجه قرار بگیرد، دقت در مدیریت و اطمینان از هویت دستگاه های اینترنت اشیاء است که در تلاش برای اتصال به شبکه و استفاده از سرویس های موجود هستند.

[1] Two-Factor Authentication (2FA)

ایمن سازی زیرساخت شبکه

شرکت ها علاوه بر دستگاه ها باید از امن بودن شبکه هایی که برای اینترنت اشیاء استفاده می شوند، مطمئن شوند. این شامل استفاده از احراز هویت قوی و مکانیسم کنترل دسترسی است، تا فقط کاربران مجاز بتوانند به شبکه ها و داده ها دسترسی داشته باشند. لذا کلمات عبور باید از پیچیدگی لازم برای جلوگیری از حملات Brute force برخوردار باشند. Brute force یک روش بیرحمانه است که کلیه ی حدس های ممکن را مورد بررسی قرار می دهد تا به کلمه ی عبور برسد. یک SNIPHERدر شبکه وجود دارد که کار رهگیری و خواندن ترافیک را در شبکه انجام می دهد. هکر می تواند الگوریتمی طراحی کند که این ترافیک را مورد بررسی قرار دهد. در صورتی که بخشی از پسورد را بیابد آن قدر حالات مختلف را مقایسه می کند تا به پسورد مورد نظر برسد. علت بیرحمی این نوع حملات ، حجم بالای عملیات مقایسه و بررسی است که انجام می دهد.

بکارگیری مکانیزم های حفاظت از داده ها

شرکت ها همچنین باید داده های اینترنت اشیاء خود را حفظ کنند. بیشتر دستگاه های متصل داده های حساس انتقالی و اطلاعات شناسایی شخصی را ذخیره می کنند؛ بنابراین محافظت از این داده ها بسیار حائز اهمیت است .شرکت هایی که در این امر مهم شکست بخورند نه تنها دچار شکست تجاری خواهند شد، بلکه ممکن است از لحاظ قانونی هم با آن ها برخورد شود . برنامه ها و داده های کاربران چه در حالت استفاده و چه زمانی که مورد استفاده قرار نمی گیرند باید رمزگذاری شوند. برای برخورداری از امنیت خوب علاوه بر سیاست های عملیات امنیتی قوی ، به برنامه های آموزشی جامع برای افراد درگیر در محیط اینترنت اشیاء لزامی است. ردیابی ممیزی گرانول، تشخیص ناهنجاری انتهایی و قابلیت پاسخگویی های قانونی امنیتی عناصری حیاتی برای اطمینان از شناسایی هر گونه نقص، قدم های اولیه پیش از گسترش صنایع اینترنت اشیاء محسوب می شوند. در نگاه اول شاید همه ی نکات گفته شده پروتکل های معمول امنیتی سایبری به نظر برسند، اما بسیاری از سازمان ها منابع و دیسیپلین لازم برای اقدامات موثر را در اختیار ندارند.

بوت امنیتی[1]

استفاده از این روش استاندارد برای امنیت اینترنت اشیاء به کاربران اطمینان می‌دهد که دستگاه مورد نظر با نرم‌افزار مورد اعتماد شرکت سازنده بوت شده است. این روش برای تشخیص دستکاری در بوت لودرها، فایل های کلیدی سیستم عامل و رام های آپشن غیرمجاز با اعتبارسنجی امضای دیجیتال آنها طراحی شده است.

مدیریت چرخه عمر امنیتی

این سیستم‌های مدیریتی بستر ارائه هر چه بهتر خدمات امنیتی را فراهم می‌نمایند. به طور مثال سیستم OTA[2] که هنگام درگیری‌های امنیتی اینترنت اشیاء اجازه می‌دهد که با کمترین میزان اختلال حملات سایبری بازیابی شوند. تمام عملیات بی سیمی که در شبکه بدون استفاده از کابل انجام شود را OTA می‌گویند.

پویش آسیب‌پذیری

یکی از راه‌های تامین امنیت سایبری در اینترنت اشیاء، بررسی و پویش آسیب‌پذیری‌ها در دستگاه‌های اینترنت اشیاء است. این بررسی‌ها می‌تواند در قالب آزمون نفوذ (Penetration Testing) یا از طریق ابزارهای خاص مانند نرم‌افزارهای پویش آسیب‌پذیری صورت بگیرد.

مدیریت دسترسی

مدیریت دسترسی نیز به عنوان یکی از روش‌های افزایش امنیت در اینترنت اشیاء استفاده می‌شود. این بدان معناست که باید دسترسی به دستگاه‌های مختلف محدود شود تا در صورت تخریب و یا هک شدن، تاثیر کمتری بر شبکه بگذارند. این کار با استفاده از فایروال‌های شبکه و سیستم‌های کنترل دسترسی انجام می‌شود.

در پایان لازم به ذکر است، با وجود تلاش‌های بسیار ایمن سازی آسیب پذیری‌ها و شکاف‌ها در حوزه امنیت سایبری اینترنت اشیاء یک امر اجتناب ناپذیر است. در سامانه‌های اینترنت اشیاء گستره وسیع، با پیچیده شدن سامانه به دلیل گوناگون بودن دیوایس‌ها، اپلیکیشن‌ها، سرویس‌ها و پروتکل‌های ارتباطی، به سختی می‌توان تشخیص داد که حادثه ای اتفاق افتاده است. لذا، لازم است امنیت به طور پیش فرض درنظر بگیرید و آن را اعمال کنید. یعنی از ویژگی‌های امنیتی که توسط امن ترین تنظیماتشان در تمامی زمان‌ها که شامل قبل، در حین و بعد از توسعه می‌باشد، پیکربندی شده‌اند، استفاده کنید. این کار به شما این امکان را می‌دهد که بتوانید حریم خصوصی و صحت داده‌ها را در هنگام انتقال حجم بالای داده‌ها و یا استفاده ی بسیار سنگین از سرویس‌ها و اپلیکیشن‌ها حفظ کنید. مانیتورینگ ارتباطات شبکه و گزارش گیری اتفاقات برای ناهنجاری ها، تست نفوذ و هک قانونی برای نشان دادن آسیب پذیری‌ها و اعمال تحلیل‌های امنیتی برای شناسایی و آگاهی از رخ دادن حوادث استراتژی‌های دیگری برای تشخیص آسیب پذیری‌ها و شکاف‌ها هستند. مدل سازی تحلیل‌ها یکی از رویکردهایی است که برای پیش بینی مسائل امنیتی به کار می‌رود. دیگر رویکردها عبارتند از: اعمال مانیتورینگ و ابزارهای تحلیلی برای همگن کردن وقایع و نمایش دادن تهدیدهای آشکار شده به طور آنی، اعمال هوش مصنوعی برای تغییر استراتژی‌های امنیتی به طور تطبیقی با توجه به تاثیرات اقدامات قبلی. اتخاذ یک پلتفرم اینترنت اشیاء که امنیت را به طور پیش

[1] Secure Boot

[2] Over-The-Air

فرض محیا، پایش و بروزرسانی می‌کند، می‌تواند در حل مشکلات امنیتی و محافظتی کمک شایانی بنماید.

نتیجه گیری

اینترنت اشیاء مفهومی رایانشی برای توصیف آینده ای که در آن اشیاءی فیزیکی، یکی پس از دیگری به اینترنت وصل می شوند و با اشیاءی دیگر در ارتباط قرار گرفته و با شناسه های منحصر به فرد و توانایی انتقال داده ها بر روی یک شبکه، با یکدیگر تعامل برقرار می کنند. با رشد این شبکه، چالشهای امنیتی جدیدی بروز پیدا می کند. امنیت سایبری اینترنت اشیاء، یک چالش عظیم برای سازمان‌هایی است که این فناوری را پیاده‌سازی می‌کنند؛ بنابراین بهینه سازی مداوم امنیت باید در اولویت قرار گیرد. سازمان‌هایی که امنیت اینترنت اشیاء خود را به عنوان یک رکن اساسی در نظر می‌گیرند، قادر خواهند بود تا بر روی اهداف اصلی اینترنت اشیاء تمرکز کنند، فرآیندها را بهینه‌سازی کنند، کیفیت خدمات را بهتر کرده، هزینه‌ها را کاهش دهند و در نهایت تجربه مشتری را بهبود ببخشند. پیش‌بینی می‌شود در آینده اینترنت اشیاء و دستگاه‌های کنترل صنعتی/عملیاتی بیش از پیش و بصورت گسترده در زندگی ما حضور داشته باشند. لذا کارشناسان امنیت سایبری وظیفه دارند که اطمینان حاصل کنند این دستگاه‌ها بدون ایجاد مشکلات امنیتی، به ما در انجام تعاملات تجاری و بهبود زندگی کمک می‌کنند. اتخاذ رویکردهای چند لایه ای امنیت در طراحی یک امر ضروری در توسعه ی اینترنت اشیاء برای مدیریت امن دیوایس‌ها، داده ها و اپلیکیشن‌های تلفن همراه و ابری و سرویس ها می‌باشد؛ همان طور که مقابله با تهدیدها و مشکلاتی که رخ می‌دهند از اهمیت ویژه ای برخوردار است. در این مقاله، ابعاد مهم امنیت سایبری در حوزه اینترنت اشیاء و راهکارهای مرتبط بررسی شد.

منابع

[1] Oracevic A, Dilek S, Ozdemir S. Security in internet of things: A survey. In2017 international symposium on networks, computers and communications (ISNCC) 2017 May 16 (pp. 1-6). IEEE.

[2] Mosenia A, Jha NK. A comprehensive study of security of internet-of-things. IEEE Transactions on emerging topics in computing. 2016 Sep 7;5(4):586-602.

[3] Mahmoud C, Aouag S. Security for internet of things: A state of the art on existing protocols and open research issues. InProceedings of the 9th international conference on information systems and technologies 2019 Mar 24 (pp. 1-6).

[4] Adat V, Gupta BB. Security in Internet of Things: issues, challenges, taxonomy, and architecture. Telecommunication Systems. 2018 Mar;67:423-41.

[5] Abomhara M, Køien GM. Cyber security and the internet of things: vulnerabilities, threats, intruders and attacks. Journal of Cyber Security and Mobility. 2015 May 22:65-88.

[6] Sadique KM, Rahmani R, Johannesson P. Towards security on internet of things: applications and challenges in technology. Procedia Computer Science. 2018 Jan 1;141:199-206.

[7] Aldowah H, Ul Rehman S, Umar I. Security in internet of things: issues, challenges and solutions. InRecent Trends in Data Science and Soft Computing: Proceedings of the 3rd International Conference of Reliable Information and Communication Technology (IRICT 2018) 2019 (pp. 396-405). Springer International Publishing.

[8] Florea I, Ruse LC, Rughinis R. Challenges in security in Internet of Things. In2017 16th RoEduNet Conference: Networking in Education and Research (RoEduNet) 2017 Sep 21 (pp. 1-5). IEEE.

[9] Weber RH, Studer E. Cybersecurity in the Internet of Things: Legal aspects. Computer Law & Security Review. 2016 Oct 1;32(5):715-28.

[10] Li F, Shi Y, Shinde A, Ye J, Song W. Enhanced cyber-physical security in internet of things through energy auditing. IEEE Internet of Things Journal. 2019 Feb 14;6(3):5224-31.

[11] Tayyaba S, Khan SA, Tariq M, Ashraf MW. Network security and Internet of things. InIndustrial Internet of Things and Cyber-Physical Systems: Transforming the Conventional to Digital 2020 (pp. 198-238). IGI Global.

[12] Raimundo RJ, Rosário AT. Cybersecurity in the internet of things in industrial management. Applied Sciences. 2022 Feb 2;12(3):1598.

[13] Ghadeer H. Cybersecurity issues in internet of things and countermeasures. In2018 IEEE International Conference on Industrial Internet (ICII) 2018 Oct 21 (pp. 195-201). IEEE.

[14] Lu Y, Da Xu L. Internet of Things cybersecurity research: A review of current research topics. IEEE Internet of Things Journal. 2018 Sep 12;6(2):2103-15.

[15] Nam D, Sukhomlin V. On cybersecurity of the Internet of Things systems. International Journal of Open Information Technologies. 2023 Feb 1;11(2):85-97.

[16] Matheu SN, Hernandez-Ramos JL, Skarmeta AF, Baldini G. A survey of cybersecurity certification for the internet of things. ACM Computing Surveys (CSUR). 2020 Dec 6;53(6):1-36.

[17] Djenna A, Harous S, Saidouni DE. Internet of things meet internet of threats: New concern cyber security issues of critical cyber infrastructure. Applied Sciences. 2021 May 17;11(10):4580.

[18] Ghimire B, Rawat DB. Recent advances on federated learning for cybersecurity and cybersecurity for federated learning for internet of things. IEEE Internet of Things Journal. 2022 Feb 10;9(11):8229-49.

[19] Abdullah A, Hamad R, Abdulrahman M, Moala H, Elkhediri S. CyberSecurity: a review of internet of things security issues, challenges and techniques. In2019 2nd International Conference on Computer Applications & Information Security (ICCAIS) 2019 May 1 (pp. 1-6). IEEE.