

راهنمای کاربری چک لیست امنیت اینترنت اشیا

مرکز هماهنگی JPCERT

ترجمه شده توسط : علی صادق الوعد

محتوا

1	مقدمه
3	2. مروری بر چک لیست و زمان استفاده از آن
3	1.2. مروری بر چک لیست
3	1.1.2. اجزاء
3	2.1.2. مروری بر نحوه استفاده از چک لیست
4	3.1.2. ساختار سیستم اینترنت اشیا و اصول اولیه
5	2.2. زمان استفاده از چک لیست
5	1.2.2. زمان استفاده توسط توسعه دهندگان محصول و مزایای مورد انتظار
6	2.2.2. زمان استفاده توسط کاربران محصول و مزایای مورد انتظار
7	3. نحوه استفاده از چک لیست
7	1.3. چگونه توسعه دهندگان محصول باید از چک لیست استفاده کنند
7	1.1.3. ساختار چک لیست
8	3.1.2. نحوه استفاده از چک لیست
9	3.1.3. مثال کاربردی
9	1.3.1.3. درباره محصولاتی که باید با چک لیست امنیت اینترنت اشیا ارزیابی شوند
10	2.3.1.3. اعمال چک لیست در سیستم جمع آوری اطلاعات تولید کارخانه
12	2.3. چگونه کاربران محصول باید از چک لیست استفاده کنند
12	1.2.3. نام هر مورد
13	2.2.3. نحوه استفاده از چک لیست
15	3.2.3. مثال کاربردی
15	1.3.2.3. درباره محصولاتی که باید با چک لیست امنیت اینترنت اشیا ارزیابی شوند
16	2.3.2.3. اعمال چک لیست برای دوربین شبکه
18	4. ارتباط بین چک لیست و سایر راهنماها
19	تشکر و قدردانی
20	مراجع

1-مقدمه

اینترنت اشیا (IoT) مفهومی است که به سیستم توزیع شده ای اشاره دارد که شامل شبکه ای از برنامه های نظارتی است که اطلاعات مربوط به وضعیت اشیاء فیزیکی را جمع آوری می کند و برنامه هایی را کنترل می کند که وضعیت اشیاء را بر اساس اطلاعات جمع آوری شده و سایر عناصر تغییر می دهند. یکی از کاربردهای این مفهوم ممکن است شامل ارائه قابلیت های ارتباطی جدید به دستگاه هایی باشد که دمای تجهیزات تولیدی را اندازه گیری و کنترل می کنند، و ایجاد سیستمی که آنها را به یک شبکه متصل می کند و از خدمات ابری و غیره استفاده می کند تا جمع آوری و تجمیع کارآمد را ممکن کند. اطلاعات تولید در یک کارخانه بزرگ دستگاه هایی که به تازگی به قابلیت های ارتباطی مجهز شده اند، مانند این مثال، اغلب «دستگاه های اینترنت اشیا» نامیده می شوند. اخیراً سیستم هایی که با دستگاه های IoT بر اساس مفهوم اینترنت اشیا ساخته شده اند توجه زیادی را به خود جلب کرده اند و انتظار می رود در سال های آینده به سرعت گسترش پیدا کنند.

به عنوان مثال، طبق گفته وزارت امور داخلی و ارتباطات [1]، با توجه به تعداد زیاد گوشی های هوشمند، تجهیزات ارتباطی و سایر دستگاه های مشابه در حال استفاده از سال 2017، تعداد دستگاه های IoT در سراسر جهان به روند صعودی خود ادامه خواهد داد. رشد سریع پیش بینی شده در حوزه های مختلف، از جمله: خودروها و تجهیزات حمل و نقل، که انتظار می رود شاهد پذیرش فزاینده اینترنت اشیا از طریق محبوبیت خودروهای متصل باشیم. مراقبت های بهداشتی، که شاهد گسترش بازار مراقبت های بهداشتی دیجیتال است. و کاربردهای صنعتی (کارخانه ها، زیرساخت ها و تدارکات)، که در آن تعداد کارخانه های هوشمند و شهرهای هوشمند در حال افزایش است.

در همین حال، دستگاه های اینترنت اشیا و همچنین سیستم هایی که بر اساس مفهوم اینترنت اشیا ساخته شده اند، به طور مداوم به یک شبکه متصل می شوند و در بسیاری از موارد، دستگاه های اینترنت اشیا متعددی از همان نوع به یک شبکه متصل می شوند که اغلب اطمینان از کنترل امنیتی را دشوار می کند. دستگاه های IoT منفرد

روترهای باند پهن برای مصرف کنندگان عمومی با وضعیت مشابه دستگاه های IoT روبرو هستند، زیرا دستگاه های بی شماری دائماً به یک شبکه متصل هستند و تضمین کنترل امنیتی را دشوار می کند. در واقع، از حدود

سال 2016 تعداد زیادی از حوادث امنیتی مربوط به روترهای پهنای باند آلوده به بدافزار Mirai گزارش شده است. دستگاه‌هایی با مدیریت نادرست مانند دستگاه‌هایی که با وصله‌های امنیتی برای رفع آسیب‌پذیری‌ها به‌روزرسانی نشده‌اند، و دستگاه‌هایی که با احراز هویت دقیق پیکربندی نشده‌اند. تنظیمات کنسول مدیریت مستعد ابتلا به بدافزار Mirai هستند. بدافزارهای مشابهی که دستگاه‌های اینترنت اشیا را هدف قرار می‌دهند، ممکن است پس از گسترش گسترده این دستگاه‌ها ظاهر شوند و نگرانی‌هایی در مورد آسیب‌های مشابه ناشی از عفونت ایجاد کنند.

برای اطمینان از عملکرد ایمن اینترنت اشیا و سایر دستگاه‌ها به طوری که می‌توان از اینترنت اشیا به طور ایمن استفاده کرد، خود این دستگاه‌ها باید با ریشه کن کردن آسیب‌پذیری‌ها و سایر اقدامات در برابر حملات ایمن شوند.

با این حال، توسعه دهندگان دستگاه‌های IoT اغلب تمرکز بیش از حد بر ایجاد عملکردهای جدید دارند و فراموش می‌کنند که روی طراحی امنیتی کار کنند، مانند مورد روترهای باند پهن آلوده به Mirai. این وضعیت را می‌توان با ارائه یک چک لیست امنیتی که به راحتی می‌تواند برای بررسی عملکردهای امنیتی دستگاه‌های IoT استفاده شود و توسعه دهندگان از آنها در هنگام طراحی دستگاه‌ها استفاده کنند، بهبود می‌یابد.

همچنین، هنگامی که کاربران سیستمی را با استفاده از دستگاه‌های اینترنت اشیا می‌سازند، انتخاب محصولات تشکیل‌دهنده‌ای که ویژگی‌های امنیتی لازم را ارائه می‌کنند، مهم است. اگر کاربران محصول نامناسبی را انتخاب کنند، ممکن است در معرض حملات سایبری قرار گیرد و از عملکرد سیستم مطابق انتظار جلوگیری می‌کند یا سیستم را قادر می‌سازد تا به عنوان سکوی پرشی برای حملات سایبری علیه اشخاص ثالث استفاده شود. با این حال، کاربران تمایل دارند روی اجرای عملکردهای اصلی تمرکز کنند و به پروژه اجازه می‌دهند بدون توجه کافی به ویژگی‌های امنیتی ادامه یابد. همچنین می‌توان با ارائه چک لیستی که به راحتی می‌تواند برای بررسی عملکردهای امنیتی دستگاه‌های اینترنت اشیا و تشویق کاربران به استفاده از آنها در هنگام ساختن سیستم‌ها استفاده شود، از این وضعیت جلوگیری کرد.

برای رسیدگی به این مسائل، (JPCERT/CC) در حال انتشار یک چک لیست امنیتی اینترنت اشیا (از این پس، «چک لیست») است که با همکاری کارگروه امنیت اینترنت اشیا انجمن امنیت شبکه ژاپن (JNSA) و دانشگاه ناگازاکی توسعه یافته است. چک لیست ساده و کاربردی طراحی شده است تا توسعه دهندگان و کاربران دستگاه

های اینترنت اشیا بتوانند به راحتی از آن استفاده کنند. اقلام چک محدود شدند تا فقط موارد اساسی و ضروری را شامل شوند و در فهرستی سازماندهی شدند که توضیح می‌دهد چه چیزی و چرا باید بررسی شود.

در این چک لیست، مواردی که باید توسط توسعه دهندگان و کاربران بررسی شود، در کنار هم برای هر آیتم چک لیست شده است. ما این قالب را انتخاب کردیم تا توسعه دهندگان دستگاه های اینترنت اشیا بتوانند نگرانی های کاربران را در نظر بگیرند و کاربران به ملاحظات توسعه دهندگان توجه کنند تا افکار آنها برای کمک به استفاده ایمن از اینترنت اشیا همگرا شود.

از آنجایی که ما چک لیست را تا حد امکان ساده کردیم، ممکن است در ابتدا نحوه استفاده از آن مشخص نباشد. بنابراین ما این کتابچه راهنمای کاربر را برای ارائه توضیحات لازم آماده کردیم. فصل 2 یک نمای کلی از چک لیست ارائه می دهد، فصل 3 نحوه استفاده از چک لیست را در حین ارائه مثال ها توضیح می دهد، و فصل 4 رابطه بین چک لیست و سایر راهنماها را روشن می کند. لطفاً این کتابچه راهنمای کاربر را بخوانید تا به شما در درک نحوه استفاده از چک لیست کمک کند.

2- مروری بر چک لیست و زمان استفاده از آن

1.2 مروری بر چک لیست

1.1.2 اجزاء

چک لیست 39 عملکرد ضروری امنیتی را فهرست می کند که کل سیستمی را که بر اساس مفهوم اینترنت اشیا (از این پس "سیستم اینترنت اشیا") ساخته شده است را قادر می سازد حتی در محیطی که تهدیدات وجود دارد، به طور ایمن به کار گرفته شود، همراه با اطلاعات پس زمینه در مورد اینکه چرا آنها ضروری هستند. این لیست برای استفاده در هنگام توسعه و استقرار محصولاتی که یک سیستم اینترنت اشیا را تشکیل می دهند طراحی شده است.

با استفاده از این چک لیست برای ارزیابی یک سیستم اینترنت اشیا که در حال توسعه است یا برای استقرار برنامه ریزی شده است، می توان تعیین کرد که آیا عملکردهای لازم برای اطمینان از امنیت سیستم اینترنت اشیا ارائه شده است یا خیر، و مواردی را که نیاز به بررسی بیشتر دارد شناسایی کرد.

چک لیست از اجزای زیر تشکیل شده است.

(1) چک لیست امنیت اینترنت اشیا

فهرستی از 39 مورد بررسی برای اطمینان از تجهیز دستگاه به عملکردهای امنیتی مورد نیاز برای یک سیستم اینترنت اشیا

(2) نمودارهای تصویری چک لیست بررسی امنیت اینترنت اشیا

مجموعه ای از نمودارها برای کمک به نشان دادن موارد بررسی در چک لیست امنیت اینترنت اشیا

(3) راهنمای کاربر چک لیست امنیت اینترنت اشیا (این سند)

راهنمای کاربر در مورد نحوه استفاده از چک لیست امنیت اینترنت اشیا

2.1.2 . مروری بر نحوه استفاده از چک لیست

از چک لیست برای ارزیابی عملکردهای امنیتی در چهار مرحله زیر استفاده کنید.

مرحله 1: موارد اولیه موجود در دستگاه اینترنت اشیا مورد ارزیابی را تعیین کنید

تعیین کنید که دستگاه IoT مورد نظر مجهز به کدام ابزارهای اولیه است. توجه داشته باشید که یک دستگاه ممکن است چندین نسخه اولیه داشته باشد. برای جزئیات بیشتر در مورد اولیه ها به 3.1.2 مراجعه کنید.

مرحله 2: مواردی که باید ارزیابی شوند را تعیین کنید

39 عملکرد امنیتی مورد نیاز در یک دستگاه اینترنت اشیا را می توان در هشت دسته دسته بندی کرد: «مدیریت کاربر»، «مدیریت نرم افزار»، «مدیریت امنیت»، «کنترل دسترسی»، «غیر مجاز»

اتصال، «رمزگذاری»، «تنظیمات سیستم» و «اعلان» — اما چک لیست را می توان برای ارزیابی تنها برخی از این دسته ها استفاده کرد. در این مرحله دسته بندی هایی را که می خواهید ارزیابی کنید انتخاب کنید. اگر می خواهید همه موارد را ارزیابی کنید، همه دسته ها را انتخاب کنید.

مرحله 3: مواردی که باید بررسی شوند را استخراج کنید

فقط موارد مربوط به موارد اولیه تعیین شده در مرحله 1 و دسته بندی های انتخاب شده در مرحله 2 را بگذارید و همه موارد دیگر را از چک لیست حذف کنید.

مرحله 4: عملکردهای امنیتی را ارزیابی کنید

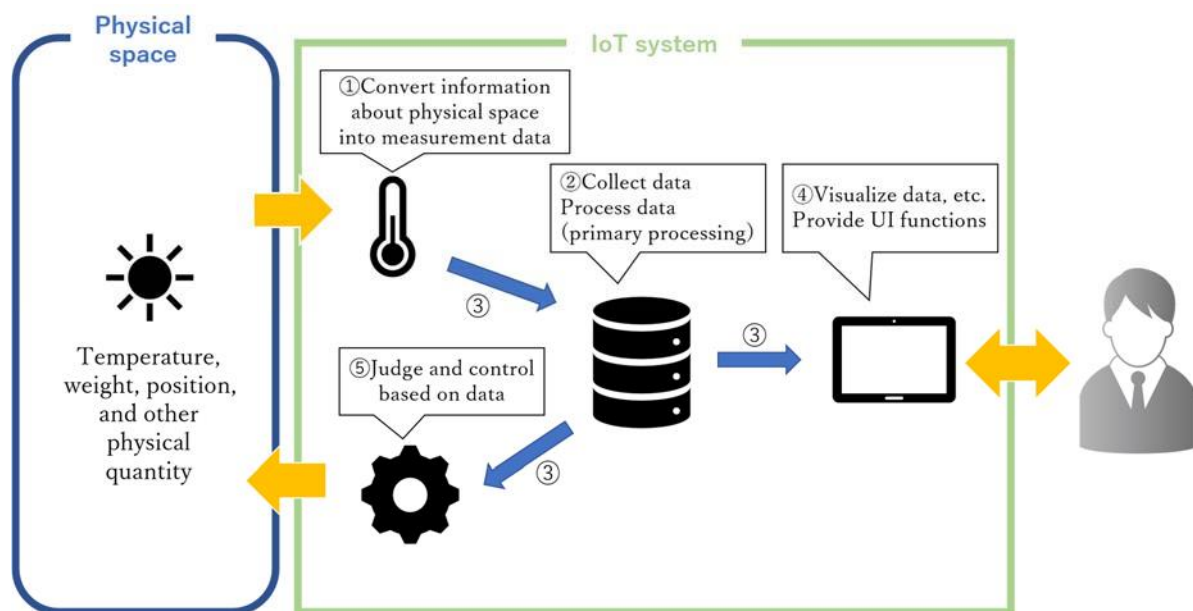
ارزیابی را با توجه به موارد چک لیست استخراج شده در مرحله 3 و ارجاع به نمودارهای تصویری چک لیست امنیت اینترنت اشیا انجام دهید.

نحوه استفاده از چک لیست را با جزئیات بیشتر در فصل 3 توضیح خواهیم داد.

3.1.2 ساختار سیستم اینترنت اشیا و اصول اولیه

در این بخش، در مورد موارد اولیه تعیین شده در مرحله 1 هنگام استفاده از چک لیست صحبت خواهیم کرد.

چک لیست سیستم های اینترنت اشیا را با توجه به عملکردها و نقش ها به منظور مشاهده عمومی به عناصر مختلف تقسیم می کند. این عناصر تشکیل دهنده به عنوان اولیه شناخته می شوند. یک سیستم اینترنت اشیا به طور کلی می تواند به ساختار نشان داده شده در [شکل 1] تقسیم شود، با توجه به اینکه برای جمع آوری اطلاعات در فضای فیزیکی و کنترل اشیاء برای تغییر وضعیت آنها بر اساس اطلاعات جمع آوری شده طراحی شده است.



[شکل 1: نحوه عملکرد سیستم های اینترنت اشیا]

① وضعیت فضای فیزیکی را اندازه گیری می کند و آن را به داده های اندازه گیری تبدیل می کند که توسط ② جمع آوری، پردازش و پردازش می شود. کاربران می توانند به داده های ذخیره شده در ② دسترسی پیدا کرده و پیکربندی کنند، اما رابط مورد استفاده برای این منظور توسط ④، ⑤ ارائه می شود تا وضعیت اشیاء را بر اساس داده های ذخیره شده در ② تغییر دهد. از آنجایی که این توابع در شبکه توزیع می شوند، یک تابع ارتباطی ③ نیز برای اتصال آنها مورد نیاز است. به دنبال مثال NIST SP800-183، چک لیست به ① به عنوان حسگر، ② به عنوان تجمیع کننده، ③ به عنوان کانال های ارتباطی، ④ به عنوان ابزارهای الکترونیکی، ⑤ به عنوان محرک

های تصمیم گیری، و بلوک‌های ساختمانی (① تا ⑤) که یک سیستم اینترنت اشیا را به صورت اولیه تشکیل می‌دهند.

سنسور	سنسور عملکرد یا وسیله ای برای اندازه گیری دما، شتاب، وزن، صدا، موقعیت ها و غیره
جمع کننده	عملکرد یا وسیله ای برای جمع آوری داده های گرفته شده توسط حسگرها
کانال ارتباطی	یک مسیر یا شبکه ارتباطی برای ارسال و دریافت داده ها
گوشی های هوشمند، رایانه های شخصی	یک رابط برای مشاهده داده ها و پیکربندی تنظیمات
ماشه تصمیم	تابعی برای محاسبه داده ها و راه اندازی یک عمل بر اساس نتیجه

توجه داشته باشید که شکل 1 یک نمودار ساده شده است و سیستم‌های IoT واقعی ممکن است دارای چندین حسگر باشند، دارای تجمیع‌کننده‌ها و ابزارهای الکترونیکی باشند که در لبه‌ها و محیط‌های ابری توزیع شده‌اند و اشکال مختلف دیگری به خود بگیرند. محرک‌های تصمیم‌گیری در سیستم‌های اینترنت اشیا که فقط داده‌ها را جمع‌آوری می‌کنند و عملکردهای کنترلی ندارند، وجود ندارند.

دستگاه‌های اینترنت اشیا که با این چک لیست ارزیابی می‌شوند باید حداقل یکی از این موارد اولیه را داشته باشند. توابع امنیتی مورد نیاز بسته به اینکه کدام موارد اولیه بر روی دستگاه اینترنت اشیا پیاده‌سازی شده‌اند متفاوت است، بنابراین موارد اولیه باید به درستی شناسایی شوند.

2.2. زمان استفاده از چک لیست

1.2.2 زمان استفاده توسط توسعه‌دهندگان محصول و مزایای مورد انتظار

زمانی که: (الف) از چک لیست استفاده کنید تا بررسی کنید که آیا عملکردهای امنیتی لازم هنگام در نظر گرفتن عملکردهای اساسی در مرحله برنامه ریزی یا مرحله طراحی اولیه یک سیستم اینترنت اشیا یا محصول تشکیل دهنده آن گنجانده شده است یا خیر. منافع مورد انتظار: - با استفاده از چک لیست در مراحل اولیه توسعه محصول، می‌توان به طور سیستماتیک بررسی کرد که آیا عملکردهای امنیتی ضروری ارائه شده است و هر گونه مشکل را زودتر اصلاح

کرد. - می توان استاندارد برای عملکردهای امنیتی برای ارائه به یک محصول ایجاد کرد و این استاندارد را می توان برای سایر محصولات توسعه یافته توسط شرکت اعمال کرد تا سطح خاصی از امنیت را تضمین کند. - مشکلات را می توان در مراحل اولیه شناسایی کرد که باعث کاهش میزان کار مجدد در فرآیند توسعه و همچنین خطر انتشار یک محصول بدون تمام عملکردهای امنیتی لازم و مستعد شدن کاربر در برابر حملات سایبری می شود.

2.2.2 زمان استفاده توسط کاربران محصول و مزایای مورد انتظار

زمانی که:

(الف) هنگام ساختن یک سیستم اینترنت اشیا با ترکیب محصولات موجود، هنگامی که محصولات نامزد محدود شدند، از چک لیست استفاده کنید تا ببینید آیا آنها به طور کامل به عملکردهای امنیتی لازم مجهز هستند یا خیر. (ب) از چک لیست برای تأیید اینکه هر محصول تشکیل دهنده یک سیستم اینترنت اشیا موجود عملکردهای امنیتی لازم را اجرا می کند استفاده کنید. اگر مشخص شد که عملکردی وجود ندارد، اقدامات متقابلی مانند افزودن تجهیزات جدید را در نظر بگیرید. منافع مورد انتظار: - (الف): با انتخاب محصولاتی که کاملاً مجهز به عملکردهای امنیتی هستند، می توان خطر حملات سایبری را کاهش داد. - (B): با شناسایی عملکردهایی که یک سیستم IoT موجود فاقد آن است و جبران شکاف با اقدامات اضافی، می توان سیستم را با تمام عملکردهای امنیتی لازم اداره کرد و خطر حملات سایبری را کاهش داد.

3. نحوه استفاده از چک لیست

1.3. چگونه توسعه دهندگان محصول باید از چک لیست استفاده کنند

1.1.3. ساختار چک لیست

چک لیست در یک جدول سازماندهی شده است که در [شکل 2] نشان داده شده است. هر ردیف از جدول مربوط به آیتم های چک جداگانه است و از نه ستون تشکیل شده است که در [جدول 1] نشان داده شده است.

				① No.	② Primitive	③ Category	④ Item	⑤ Purpose of this item	⑥ To be checked by developers	⑦ To be checked by users	⑧ Result	⑨ Comment
Item	Primitive	Category	Item	Purpose of this item	To be checked by developers	To be checked by users	Result	Comment				
1	○	○	○	Account lockout mechanism	Prevent improper operation of the device by a third party	Provide a function for locking the account and preventing login when evidence of multiple consecutive login failures has occurred.	Check available account control settings, and check that the account is locked as configured.					
2	○	○	○	Option to force-expire accounts not used for a certain period of time	Prevent login from accounts not used for a certain period of time	Provide a function for locking an account that has elapsed a set expiration period.	Check that accounts expire at the end of the expiration period.					
3	○	○	○	Function for ensuring password strength	Prevent unauthorized login by brute force, dictionary, and other attacks	Provide a function for allowing only passwords that meet certain conditions, such as the use of mixing the upper, lower, and numeric characters.	Check that passwords that do not meet the required conditions cannot be registered.					
4	○	○	○	Password security options (two-factor authentication, etc.)	Make it difficult for a third party to log in to the system	Check the use of password security options, e.g., two-factor authentication.	Check that password security options can be used.					
5	○	○	○	Permission management for accounts used to launch services and processes	Restrict permissions for launching services and processes by resource, and lower the scope of impact when an incident occurs	Do not require a supervisor when launching services and processes.	Check that the system operates with a dedicated user for services and processes.					
6	○	○	○	Shared user account	Enable the assignment of appropriate permissions according to job	Provide an account management function.	Check that a shared account is used with appropriate permissions and scope of privilege.					
7	○	○	○	Assignment of appropriate permissions to administrative users	Enable administrative users to use necessary permissions	Provide a function for managing permissions.	Check that administrative users are assigned appropriate permissions.					
8	○	○	○	Function for assigning permissions to general users	Enable users to use only necessary permissions	Provide a function for assigning permissions to users.	Check that permissions can be assigned to users, and the system can be used according to assignments.					
9	○	○	○	Authorization control function	Enable the assignment of access rights according to roles	Provide a function for assigning access rights according to the use of an account.	Check that information and functions that are not authorized cannot be used.					
10	○	○	○	Service linkage	Ensure login information is not relayed to other services more than necessary	Provide a function for indicating to the user the information relayed to other services when using those services.	Check what information is relayed to other services.					
11	○	○	○	Web application firewall	Enable the use of web application firewalls	Enable web application firewalls.	Check that web application firewalls can be used.					
12	○	○	○	Firewall function included with the product	Use the firewall function included with the product to increase security	Enable the firewall function included with the product.	Check that the firewall function included with the product can be used.					
13	○	○	○	Software version	Use the software version that addresses vulnerabilities, bugs, and other issues to address security	Provide a function for updating the software and a function for displaying the version.	Check that the software can be updated and the version can be checked.					
14	○	○	○	Antivirus function	Use the antivirus function included with the product to increase security	Enable the use of the antivirus function included with the product.	Check that the anti-virus function included with the product can be used.					
15	○	○	○	Improper data processing	Prevent unintended system operations	Provide a function for restricting data to be accepted.	-					
16	○	○	○	Data traffic	Prevent DDoS and other attacks into consideration in designing the amount of data to be handled by the system	Provide a function for restricting the amount of data traffic to be accepted, as other similar functions.	Check the amount of data traffic to be accepted.					

شکل 2 چک لیست امنیت اینترنت اشیا

[جدول 1 عناصر چک لیست امنیت اینترنت اشیا]

شماره	نام آیتم	توضیحات
1	شماره	شماره اقلام چک
2	اولیه	اصول اولیه اینترنت اشیا در "2.1.3. ساختار سیستم اینترنت اشیا و اصول اولیه» به هر یک از موارد اولیه مربوط می شود. (S: سنسور، A: Aggregator، E: eUtility، د: ماشه تصمیم، ج: کانال ارتباطی) مواردی که باید برای هر یک از موارد اولیه بررسی شوند با دایره "O" مشخص می شوند.
3	دسته بندی	39 مورد چک در یکی از 8 دسته زیر گروه بندی می شوند: (1) مدیریت کاربر (2) مدیریت نرم افزار (3) مدیریت امنیت (4) کنترل دسترسی (5) اتصال غیرمجاز (6) رمزگذاری (7) تنظیمات سیستم (8) اعلان
4	آیتم	
5	هدف از این آیتم	الزامات امنیتی مربوط به هر مورد چک
6	برای بررسی توسط توسعه دهندگان	مواردی که باید توسط توسعه دهندگان محصول بررسی شود. نتایج بررسی را در ستون Result بنویسید
7	برای بررسی توسط توسعه کاربران	مواردی که باید توسط کاربران محصول بررسی شود. نتایج بررسی را در ستون Results بنویسید.
8	نتیجه	ستون برای نوشتن در نتایج چک
9	نظر	اگر نتیجه چک "Pass" نیست اما به این نتیجه رسیدید که مشکلی وجود ندارد، دلیل آن را در این ستون بنویسید.

2.1.3. نحوه استفاده از چک لیست

گام 2

اگر می خواهید انواع خاصی از عملکردهای امنیتی را از بین هشت دسته (مدیریت کاربر، مدیریت نرم افزار، مدیریت امنیت، کنترل دسترسی، اتصال غیرمجاز، رمزگذاری، تنظیمات سیستم و اعلان) بررسی کنید، موارد مربوطه را برای بررسی انتخاب کنید.

اگر نمی‌خواهید دسته‌های خاصی را انتخاب کنید، همه موارد را بررسی کنید.

به عنوان مثال، اگر می‌خواهید عملکردهای لازم برای کنترل دسترسی دوربین شبکه را بررسی کنید:

→ موارد شماره IV-1 تا شماره IV-4 را در دسته کنترل دسترسی بررسی کنید.

اگر می‌خواهید همه موارد را بررسی کنید:

→ شماره I-1 تا شماره VIII-2 را بررسی کنید.

مرحله 3

مواردی که باید بررسی شوند را استخراج کنید.

- فقط موارد چک با دایره "○" را برای اولیه تعیین شده در مرحله 1 انتخاب کنید. موارد بدون دایره "○" را نادیده بگیرید.

- مواردی که مطابق با (های) اولیه تعیین شده در دسته بندی های انتخاب شده در مرحله 2 هستند، توابع امنیتی هستند که باید بررسی شوند.

مرحله 4

بررسی کنید که آیا تابع توضیح داده شده در ستون "بررسی توسط توسعه دهندگان" اجرا می‌شود یا اجرا خواهد شد و در ستون "نتیجه" "Pass" یا "Fail" را بنویسید. اگر در درک توضیحات ستون "بررسی شدن توسط توسعه دهندگان" مشکل دارید، لطفاً به نمودارهای تصویری چک لیست بررسی امنیت اینترنت اشیا مراجعه کنید. اگر نتیجه بررسی برای هر موردی "شکست" بود، مواردی مانند اینکه آیا آن تابع را می‌توان پیاده سازی کرد یا با یک تابع دیگر جایگزین کرد، در نظر بگیرید و یافته ها را در ستون "نظر" بنویسید. این نظر هنگام تهیه یک سند توضیحی برای سایر طرف ها یا یک کتابچه راهنمای کاربر به عنوان یک مرجع عمل می‌کند.

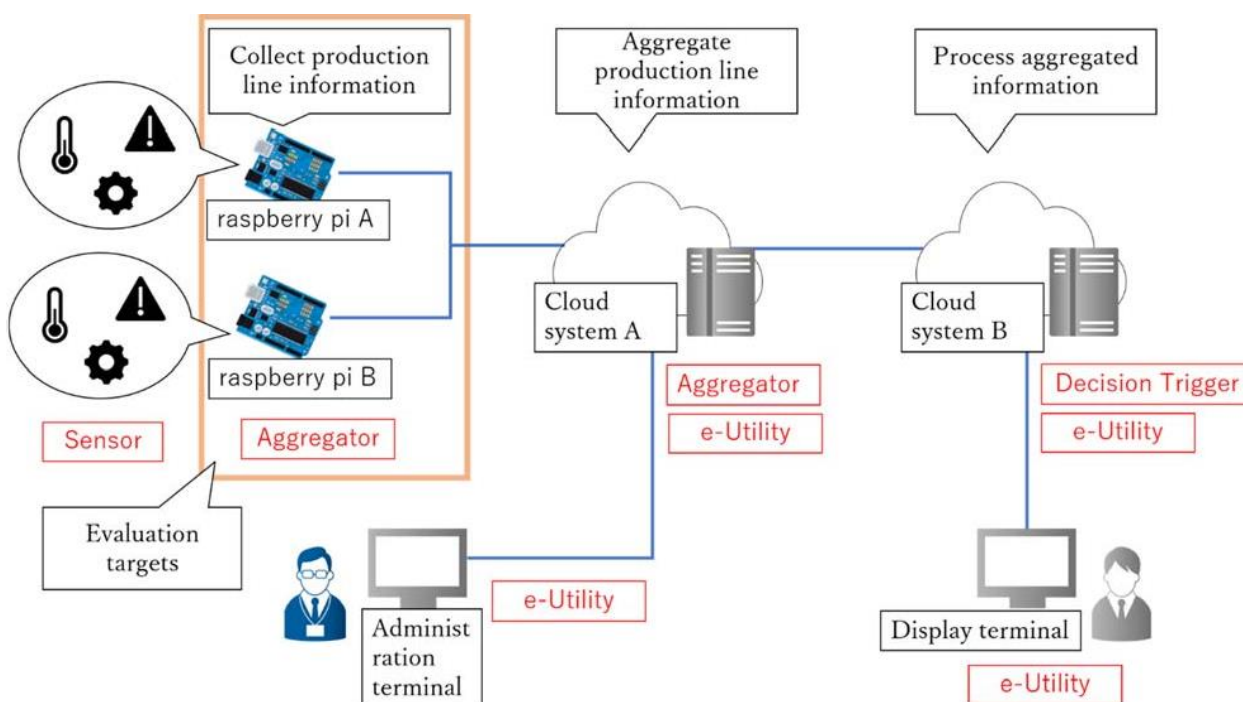
3.1.3. مثال کاربردی

به عنوان مثال موردی برای استفاده از چک لیست، موردی را مورد بحث قرار می دهیم که در آن چک لیست برای بررسی امنیت یک سیستم جمع آوری اطلاعات تولید در یک کارخانه استفاده می شود.

1.3.1.3. درباره محصولات که باید با چک لیست امنیت اینترنت اشیا ارزیابی شوند

این سیستم از Raspberry Pi برای جمع آوری اطلاعات تولید برای هر خط تولیدی که در تولید محصول P نقش دارد، استفاده می کند، اطلاعات تولید را در سیستم ابری A جمع آوری می کند، سپس اطلاعات روی سیستم ابری B را پردازش می کند تا در دستگاه های نمایش داده قابل دسترسی باشد.

[شکل 3] یک نمودار ساختاری است که سیستم را به سطوح عناصر تقسیم می کند و نوع هر عنصر به « 3.1.2. ساختار سیستم اینترنت اشیا و اصول اولیه » اشاره می کند.



[شکل 3 سیستم جمع آوری اطلاعات تولید در یک کارخانه]

در مورد این سیستم جمع‌آوری اطلاعات تولید، هر دو سیستم ابری دارای عملکرد نمایش صفحه نمایش برای کاربران هستند، بنابراین فرض می‌شود که نقش‌های اولیه چندگانه را ایفا می‌کنند (یعنی سیستم ابری A، تجمیع‌کننده و eUtility و سیستم ابری B، تصمیم‌گیری. ماشه و eUtility).

2.3.1.3. اعمال چک لیست در سیستم جمع‌آوری اطلاعات تولید کارخانه

در این مثال، Raspberry Pi A و B سیستم با استفاده از چک لیست ارزیابی شد. بر اساس مشخصات، موارد نشان داده شده در [جدول 2] به عنوان "شکست" در نظر گرفته شد.

[جدول 2 موارد قابل اجرا در چک لیست]

دسته بندی	مورد
مدیریت کاربر	گزینه های امنیتی رمز عبور (احراز هویت دو مرحله ای و غیره)
	مدیریت مجوز برای حساب های مورد استفاده برای راه اندازی خدمات و فرآیندها
	هماهنگی خدمات
مدیریت نرم افزار	عملکرد آنتی ویروس
	پردازش نادرست داده ها
	ترافیک داده
مدیریت امنیت	مدیریت جلسه (تنظیمات کوکی)
	مدیریت جلسه (بازنویسی URL)
	مدیریت جلسه (صدور شناسه جلسه هنگام ورود به سیستم و پردازش تاییدیه مهم)
کنترل دسترسی	پورت های پیش فرض برای دسترسی از راه دور
اتصال غیرمجاز	UPnP
رمزگذاری	عملکرد رمزگذاری داده ها
	روش رمزگذاری

از موارد فوق، تصمیم گرفته شد که عملکردهای زیر را اجرا نکنیم زیرا اطلاعاتی که توسط سیستم مدیریت می شود در قوانین شرکت کاملاً محرمانه تلقی نمی شود.

- مدیریت کاربر: گزینه های امنیتی رمز عبور (احراز هویت دو مرحله ای و غیره)

- رمزگذاری: عملکرد رمزگذاری داده ها

از موارد باقیمانده، به نظر می رسد که موارد زیر واقعاً قابل اجرا هستند و باید برای افزودن در نظر گرفته شوند.

- مدیریت کاربر: هماهنگی خدمات

- مدیریت نرم افزار: پردازش نادرست داده ها

- مدیریت نرم افزار: ترافیک داده ها

- مدیریت امنیت: مدیریت جلسه (تنظیمات کوکی)

- کنترل دسترسی: پورت های پیش فرض برای دسترسی از راه دور

- Encryption: روش رمزگذاری

2.3. چگونه کاربران محصول باید از چک لیست استفاده کنند

1.2.3. نام هر مورد

چک لیست در یک جدول سازماندهی شده است که در [شکل 4] نشان داده شده است. هر ردیف از جدول مربوط به آیتم های چک جداگانه است و از نه ستون تشکیل شده است که در [جدول 3] نشان داده شده است.

										① No.	② Primitive	③ Category	④ Item	⑤ Purpose of this item	⑥ To be checked by developers	⑦ To be checked by users	⑧ Result	⑨ Comment
Item	Primitive	Category	Item	Purpose of this item	To be checked by developers	To be checked by users	Result	Comment										
1	○	○	○	Account logout mechanism	Prevent improper operation of the device by a third party	Provide a function for logging the account and preventing login when evidence of multiple consecutive login failures has occurred.	Check available account control settings, and check that the account is locked as configured.											
2	○	○	○	Option to force-expire accounts not used for a certain period of time	Prevent login from accounts not used for a certain period of time	Provide a function for logging an account that has elapsed a set expiration period.	Check that accounts expire at the end of the expiration period.											
3	○	○	○	Function for ensuring password strength	Prevent unauthorized login by brute force, dictionary, and other attacks	Provide a function for allowing only passwords that meet certain conditions, such as the use of mixing the upper/lower and numbers.	Check that passwords that do not meet the required conditions cannot be registered.											
4	○	○	○	Password security options (two-factor authentication, etc.)	Make it difficult for a third party to log in to the system	Check the use of password security options, e.g., two-factor authentication.	Check that password security options can be used.											
5	○	○	○	Permission management for accounts used to launch services and processes	Restrict permissions for launching services and processes by accounts, and lower the scope of impact when an incident occurs	Do not require a supervisor when launching services and processes.	Check that the system operates with a dedicated user for services and processes.											
6	○	○	○	Shared user account	Enable the assignment of appropriate permissions according to job	Provide an account management function.	Check that a shared account is used with appropriate permissions and scope of privilege.											
7	○	○	○	Assignment of appropriate permissions to administrative users	Enable administrative users to use necessary permissions	Provide a function for managing permissions.	Check that administrative users are assigned appropriate permissions.											
8	○	○	○	Function for assigning permissions to general users	Enable users to use only necessary permissions	Provide a function for assigning permissions to users.	Check that permissions can be assigned to users, and the system can be used according to assignments.											
9	○	○	○	Authorization control function	Enable the assignment of access rights according to roles	Provide a function for assigning access rights according to the use of an account.	Check that information and functions that are not authorized cannot be used.											
10	○	○	○	Service linkage	Ensure login information is not relayed to other services more than necessary	Provide a function for indicating to the user the information relayed to other services when using those services.	Check what information is relayed to other services.											
11	○	○	○	Web application firewall	Enable the use of web application firewalls	Enable web application firewalls.	Check that web application firewalls can be used.											
12	○	○	○	Firewall function included with the product	Use the firewall function included with the product to increase security	Enable the firewall function included with the product.	Check that the firewall function included with the product can be used.											
13	○	○	○	Software version	Use the software version that addresses vulnerabilities, bugs, and other issues to improve security	Provide a function for updating the software and a function for displaying the version.	Check that the software can be updated and the version can be displayed.											
14	○	○	○	Antivirus function	Use the antivirus function included with the product to increase security	Enable the use of the antivirus function included with the product.	Check that the anti-virus function included with the product can be used.											
15	○	○	○	Improper data processing	Prevent unintended system operations	Provide a function for restricting data to be accepted.	-											
16	○	○	○	Data traffic	Prevent DDoS and other attacks into consideration in designing the amount of data to be handled by the system	Provide a function for restricting the amount of data traffic to be accepted, as other similar functions.	Check the amount of data traffic to be accepted.											

شکل 4 چک لیست امنیت اینترنت اشیا

جدول 3 عناصر چک لیست امنیت اینترنت اشیا]

شماره	نام آیتم	توضیحات
1	شماره	شماره ارقام چک
2	اولیه	اصول اولیه اینترنت اشیا در "2.1.3. ساختار سیستم اینترنت اشیا و اصول اولیه» به هر یک از موارد اولیه مربوط می شود. (S: سنسور، A: Aggregator، E: eUtility، د: ماشه تصمیم، ج: کانال ارتباطی) مواردی که باید برای هر یک از موارد اولیه بررسی شوند با دایره "O" مشخص می شوند.
3	دسته بندی	39 مورد چک در یکی از 8 دسته زیر گروه بندی می شوند: (1) مدیریت کاربر (2) مدیریت نرم افزار (3) مدیریت امنیت (4) کنترل دسترسی (5) اتصال غیرمجاز (6) رمزگذاری (7) تنظیمات سیستم (8) اعلان
4	آیتم	
5	هدف از این آیتم	الزامات امنیتی مربوط به هر مورد چک
6	برای بررسی توسط توسعه دهندگان	مواردی که باید توسط توسعه دهندگان محصول بررسی شود. نتایج بررسی را در ستون Result بنویسید
7	برای بررسی توسط کاربران	مواردی که باید توسط کاربران محصول بررسی شود. نتایج بررسی را در ستون Results بنویسید.
8	نتیجه	ستونی برای نوشتن در نتایج چک
9	نظر	اگر نتیجه چک "Pass" نیست اما به این نتیجه رسیدید که مشکلی وجود ندارد، دلیل آن را در این ستون بنویسید.

2.2.3. نحوه استفاده از چک لیست مرحله 1

تعیین کنید که محصول مورد استفاده با کدام یک از محصولات اولیه در کل سیستم اینترنت اشیا مطابقت دارد. نگاه کنید به "2.1.3. ساختار سیستم اینترنت اشیا و اصول اولیه» برای جزئیات.

به عنوان مثال، یک دستگاه پوشیدنی از نوع ساعت که قادر به اندازه‌گیری ضربان قلب و گام‌ها است، با «سنسور» مطابقت دارد، اما با «Aggregator» نیز مطابقت دارد، زیرا ضربان قلب و داده‌های مرحله را جمع‌آوری می‌کند و با یک سرور خارجی ارتباط برقرار می‌کند.

مرحله 2

اگر می‌خواهید انواع خاصی از عملکردهای امنیتی را از بین هشت دسته (مدیریت کاربر، مدیریت نرم افزار، مدیریت امنیت، کنترل دسترسی، اتصال غیرمجاز، رمزگذاری، تنظیمات سیستم و اعلان) بررسی کنید، موارد مربوطه را برای بررسی انتخاب کنید.

اگر نمی‌خواهید دسته‌های خاصی را انتخاب کنید، همه موارد را بررسی کنید.

به عنوان مثال، اگر می‌خواهید عملکردهای لازم برای کنترل دسترسی دوربین شبکه را بررسی کنید:

→ موارد شماره IV-1 تا شماره IV-4 را در دسته کنترل دسترسی بررسی کنید. اگر می‌خواهید همه موارد را بررسی کنید:

→ شماره I-1 تا شماره VIII-2 را بررسی کنید.

مرحله 3

مواردی که باید بررسی شوند را استخراج کنید.

- فقط موارد چک با دایره "O" را برای اولیه تعیین شده در مرحله 1 انتخاب کنید. موارد بدون دایره "O" را نادیده بگیرید.

- مواردی که مطابق با (های) اولیه تعیین شده در دسته بندی های انتخاب شده در مرحله 2 هستند، توابع امنیتی هستند که باید بررسی شوند.

مرحله 4

بررسی کنید که آیا محصولی که باید ارزیابی شود، با توضیحات مندرج در «برای بررسی توسط کاربران» مطابقت دارد یا خیر.

- بررسی کنید که آیا محصول به عملکردهای توضیح داده شده در "برای بررسی توسط کاربران" مجهز است یا خیر.

- مواردی را که به نمودارهای تصویری چک لیست امنیت اینترنت اشیا پیوست شده به فهرست چک امنیت اینترنت اشیا ارجاع می دهند، بررسی کنید.

برای مواردی که با توضیحات مطابقت دارند، در ستون «نتیجه» علامت بزنید و برای مواردی که مطابقت ندارند دلیل آن را در ستون «نظر» بنویسید.

- برای مواردی که علامت تیک ندارند، مواردی مانند اینکه آیا تابع می تواند در زمان توسعه اجرا شود یا با عملکرد دیگری تکمیل شود را در نظر بگیرید و یافته ها را در ستون "نظر" بنویسید تا هنگام تهیه یک سند توضیحی به عنوان مرجع استفاده شود. یک دفترچه راهنما.

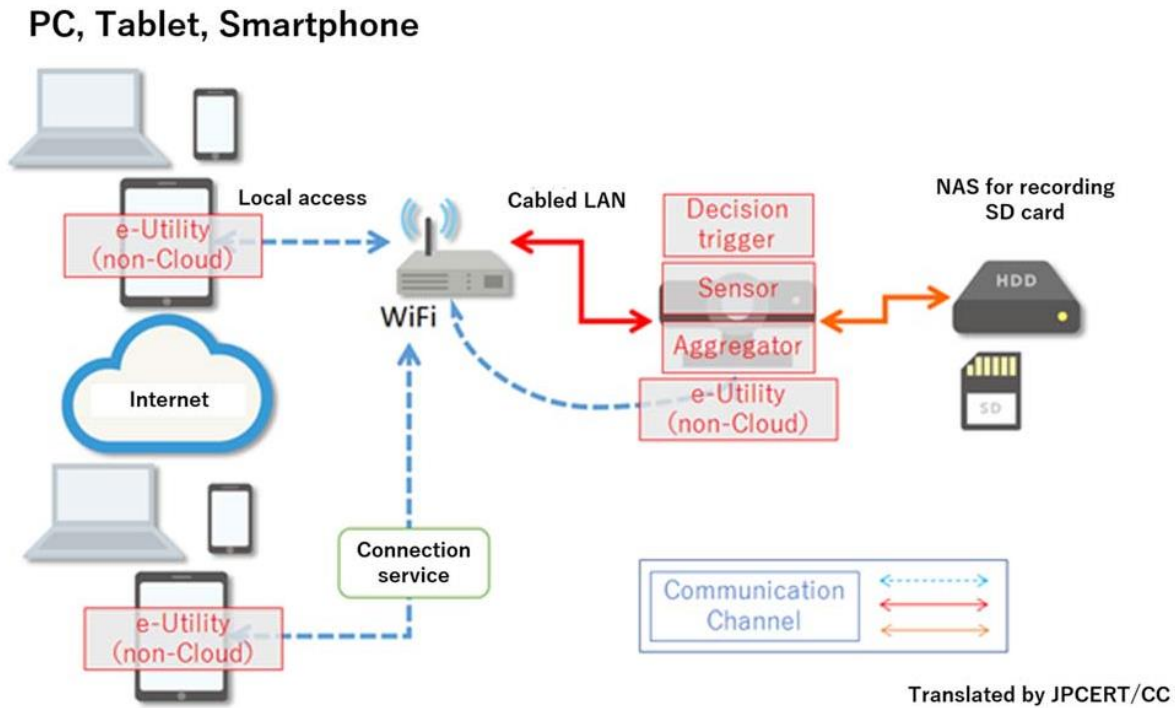
3.2.3. مثال کاربردی

به عنوان مثال موردی برای استفاده از چک لیست، موردی را مورد بحث قرار خواهیم داد که در آن کاربری که در نظر دارد یک دوربین شبکه تجاری در دسترس را به منظور نظارت از راه دور خانه خود به دلایل امنیتی معرفی کند، هنگام در نظر گرفتن اقدامات امنیتی مورد نیاز در محصول، ارزیابی انجام داد. .

1.3.2.3. درباره محصولاتی که باید با چک لیست امنیت اینترنت اشیا ارزیابی شوند

نمودار زیر پیکربندی هر یک از عملکردهای دوربین شبکه طبقه بندی شده در ارزیابی را نشان می دهد.

[شکل 5] با ارجاع به مثال دوربین وب در "راهنمای امنیت اینترنت اشیا برای مصرف کنندگان" صادر شده توسط JNSA ایجاد شده است.



[شکل 5 طبقه بندی بر اساس بدوی در مورد دوربین شبکه]

مرجع: "راهنمای امنیت اینترنت اشیا برای مصرف کنندگان"، انجمن امنیت شبکه ژاپن (JNSA)

در پیکربندی دوربین شبکه در این مثال، دوربین خود عملکردهای زیادی دارد و بنابراین می تواند چندین ویژگی اولیه را به خود اختصاص دهد.

- دوربین وب (حسگر، جمع آوری، ابزار الکترونیکی، ماشه تصمیم)

- گوشی های هوشمند، رایانه های شخصی (eUtility)

- وای فای، اتوبوس داخلی (کانال ارتباطی)

2.3.2.3. اعمال چک لیست برای دوربین شبکه

در این مثال، چک لیست برای ارزیابی بخش eUtility دوربین شبکه استفاده شد.

[جدول 4] عملکردهایی را فهرست می‌کند که دوربین شبکه‌ای که کاربر در نظر دارد معرفی کند، پس از بررسی موارد موجود در فهرست چک با راهنمای کاربر محصول، از دست رفته است.

[جدول 4 موارد قابل اجرا در چک لیست]

دسته بندی	مورد
مدیریت کاربر	امکان انقضای اجباری رمزهای عبور پس از تاریخ انقضا
	عملکردی برای اطمینان از قدرت رمز عبور
	گزینه های امنیتی رمز عبور (احراز هویت دو مرحله ای و غیره)
	مدیریت مجوز برای حساب های مورد استفاده برای راه اندازی خدمات و فرآیندها
مدیریت نرم افزار	عملکرد فایروال همراه محصول است
	عملکرد آنتی ویروس
مدیریت دسترسی	دسترسی با وسایل فیزیکی کنترل نشده
	پورت های پیش فرض برای دسترسی از راه دور
	امنیت ارتباطات بی سیم (WPS)
اتصال غیرمجاز	محدودیت پورت های شبکه
	UPnP

با توجه به نتایج فوق، سه مورد برای بحث در معرفی دوربین شبکه که مورد ارزیابی قرار گرفت انتخاب شد.

(1) بهبود عملکرد احراز هویت

عملکرد احراز هویت دوربین های شبکه اغلب با بسیاری از محصولات به اندازه کافی دقیق پیکربندی نمی شود. به عنوان مثال، محصولاتی وجود دارند که با همان رمز احراز هویت ساده برای همه دستگاه ها تنظیم شده اند و با برخی از این محصولات رمز عبور در اینترنت در دسترس است. در حالی که توسعه دهندگان باید راهی برای جلوگیری از پیکربندی دستگاه ها با رمز عبور یکسان در نظر بگیرند، آنها همچنین باید مشخصاتی را طراحی کنند که فقط اجازه تنظیم رمز عبور قوی را بدهد. همچنین ترجیح داده می شود که با اجرای احراز هویت دو مرحله ای و مواردی از این دست، احراز هویت را تقویت کنید. کاربران همچنین باید محصولاتی را انتخاب کنند که اجازه

می دهد رمز عبور قوی تنظیم شود یا آنهایی که گزینه هایی مانند احراز هویت دو مرحله ای را ارائه می دهند و محصولات را با تنظیمات مناسب پیکربندی کنند.

(2) محدودیت دسترسی خارجی

دوربین های تحت شبکه گاهی اوقات بدون اطلاع کاربر برای طرف های خارجی قابل دسترسی هستند. مهاجمان ممکن است پورت های پیش فرض چنین دستگاه هایی را برای دسترسی از راه دور هدف قرار دهند تا باعث آلودگی بدافزار شوند، بنابراین کاربران باید کنترل دسترسی خارجی یا تغییر پورت ها را برای دسترسی از راه دور در نظر بگیرند. کاربران همچنین باید توجه داشته باشند که UPnP (Universal Plug and Play) و سایر عملکردهای مشابه ممکن است برای دسترسی به یک دستگاه در یک محیط NAT از اینترنت استفاده شوند. توسعه دهندگان باید توابعی را برای کنترل دسترسی خارجی و تغییر پورت ها برای دسترسی از راه دور، و همچنین مشخصاتی که امکان غیرفعال کردن UPnP را فراهم می کنند، در نظر بگیرند.

(3) استفاده از توابع محصول موجود

در صورت وجود، استفاده از فایروال و عملکردهای ضد ویروس نیز باید به عنوان یک اقدام متقابل در نظر گرفته شود. بسته به مشخصات محصول، ممکن است اجرای این توابع به عنوان EUtilities دشوار باشد. در چنین مواردی، اجرای آنها را در جای دیگری در نظر بگیرید. مهاجمان تمایل دارند به طور مداوم به حفره های امنیتی شناخته شده حمله کنند، بنابراین توسعه دهندگان باید تابعی را برای به روز رسانی سیستم عامل برای رفع آسیب پذیری ها و غیره در هنگام انتشار اجرا کنند و کاربران باید محصولات خود را به روز نگه دارند.

4. ارتباط بین چک لیست و سایر راهنماها

موارد چک لیست بر اساس اسناد ارزیابی امنیت فناوری اطلاعات علاوه بر اسناد ارزیابی امنیت برای اینترنت اشیا ایجاد شده است. این به این دلیل است که برخی از سیستم‌های اینترنت اشیا ممکن است با استفاده از فناوری‌های IT موجود پیکربندی شوند - برای مثال، یک رابط پیاده‌سازی شده برای eUtility و غیره که در یک محصول مشخص شده است ممکن است از پروتکل ارتباطی مشابه وب استفاده کند، مانند دسترسی از طریق یک برنامه وب یا API - و ما فکر کردیم ارزیابی امنیتی طراحی شده برای IT مفید خواهد بود.

در ایجاد چک لیست، اسناد زیر را به عنوان مرجع اصلی خود انتخاب کردیم، که توضیحات مفصلی را در مورد نحوه انجام ارزیابی‌های امنیتی، از بین بسیاری از اسناد ارزیابی امنیت اینترنت اشیا در دسترس ارائه می دهد.

راهنمای امنیت اینترنت اشیا OWASP

https://www.owasp.org/index.php/IoT_Security_Guidance

استاندارد اجرای تست نفوذ

گروه استاندارد اجرای تست نفوذ

http://www.pentest-standard.org/index.php/Main_Page

ما موارد مشترک را در این دو سند شناسایی کردیم و از آنها به عنوان موارد استاندارد در بحث‌های خود استفاده کردیم. این اسناد موارد اساسی در تفکر در مورد امنیت فناوری اطلاعات و اینترنت اشیا را خلاصه می کند و بسیاری از آنها در هر دو سند پوشش داده شده است. به این دلایل، ما معتقدیم این موارد رایج توجه زیادی را به خود جلب می کنند و باید در اولویت قرار گیرند.

با این وجود، ما در این سند پیشنهاد نمی کنیم که همه این موارد الزاماتی هستند که باید انجام شوند. به عبارت دیگر، ما معتقدیم این موارد پرمخاطب، موارد توصیه شده ای هستند که نیاز به بحث و بررسی برای اقدامات اولویت دار و غیره دارند.

این به این دلیل است که محصولات و سیستم ها استانداردها و الزامات دیگری برای برآورده کردن دارند و اقلام بر اساس آن وزن می شوند. هنگام اعمال چک لیست، باید آن را همراه با سایر الزامات در نظر گرفت.

در حالی که چک لیست موارد اساسی را که باید با توجه به امنیت سیستم های اینترنت اشیا در نظر گرفته شود خلاصه می کند، برخی از مسائل ممکن است اولویت بندی راه حلی را بر اساس الزامات ایمنی به جای الزامات امنیتی تضمین کند. در این سند، ما این دیدگاه را داریم که مناسب است هم ایمنی و هم ایمنی را در نظر بگیریم. به این ترتیب، توصیه می کنیم به جای اولویت بندی هر یک، هر دو جنبه را به طور همزمان در نظر بگیرید تا اطمینان حاصل شود که اقدامات مناسب در محصولات و سیستم های نهایی گنجانده شده اند.

تشکر و قدردانی

ما بسیار مدیون آقای Masato Matsuoka، رهبر کارگروه امنیت اینترنت اشیا (JNSA)، و دکتر Masahiko Kato، استاد دانشگاه ناکازاکی هستیم، برای کمک ارزشمندشان در بررسی این سند و ایجاد چک لیست. ما همچنین از اعضای کارگروه امنیت اینترنت اشیا (JNSA) و بسیاری از همکاران دیگر برای در نظر گرفتن نکات بحث، توصیه های روشننگری دریافت کردیم. از همه کسانی که در تهیه این سند مشارکت داشتند تشکر می کنیم.

منابع

- IoT Security Guidance
OWASP
https://www.owasp.org/index.php/IoT_Security_Guidance
- The Penetration Testing Execution Standard
Penetration Testing Execution Standard Group
http://www.pentest-standard.org/index.php/Main_Page
- NIST Special Publication 800-183
Networks of 'Things NIST
<https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-183.pdf>
- NIST SP 800-160 Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems

NIST

<https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-160.pdf>

- IoT Security Guide for Consumers
Japan Network Security Association
(JNSA) <https://www.jnsa.org/result/iot/>
- Overview of the Internet of things
International Telecommunication Union
(ITU)
<https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=y.2060>
- IoT Security Guidelines (Ver 1.0)
Ministry of Economy, Trade and Industry/Ministry of Internal Affairs and Communications http://www.iotac.jp/wp-content/uploads/2016/01/IoT-Security-Guidelines_ver.1.0.pdf
- IoT Safety/Security Development Guidelines
(Second Edition) Information-technology
Promotion Agency, Japan (IPA)
<https://www.ipa.go.jp/sec/reports/20160324.html>
- The STRIDE
Threat Model
Microsoft
[https://msdn.microsoft.com/en-us/library/ee823878\(v=cs.20\).aspx](https://msdn.microsoft.com/en-us/library/ee823878(v=cs.20).aspx)
- The WASC Threat
Classification v2.0 WASC
Projects
<http://projects.webappsec.org/w/page/13246978/Threat%20Classification>
- OWASP Testing Guide v4
Table of Contents OWASP
https://www.owasp.org/index.php/OWASP_Testing_Guide_v4_Table_of_Cont