زلباس سلاح

نواع حملات، سناریوهای حمله و مکانیزم‌های مقابله

عکس: CNN

سبکی به‌طور گسترده در دستگاه‌های الکترونیکی قابل حمل، از جمله پیجرها، استفاده می‌شوند. اما این نوع باتری‌ها به تغییرات دما، ولتاژ بالا یا شارژ و دشارژ غیرمعمول حساس هستند. در این باتری‌ها عوامل کلیدی که می‌تواند به آسیب باتری منجر شود، عبارتند از: الف) شارژ بیش از حد و به‌ویژه ولتاژ بالا در زمان شارژ بیش از حد می‌تواند منجر به افزایش دما، آسیب به ساختار داخلی باتری و در نهایت باعث اشتعال یا انفجار شود. ب) تخلیه کامل و مکرر یا دشارژ شدید باتری می‌تواند به خرابی سلول‌های باتری و بی‌ثباتی شیمیایی آن منجر شود. ج) دمای بالا و افزایش دما، به‌خصوص در یک محیط بسته و بدون تهویه، می‌تواند باعث گرم شدن باتری و در نهایت انفجار شود.

در ادامه سناریوهای احتمالی برای انجام حمله روی باتری‌های لیتیومی بررسی شده است.

دستکاری نرم‌افزاری سیستم مدیریت باتری (BMS)[۱۲]

در دستگاه‌های الکترونیکی پیشرفته مانند گوشی‌های هوشمند، لب‌تاپ‌ها و برخی از پیجرها، یک سیستم مدیریت باتری (BMS) وجود دارد که وظیفه کنترل و تنظیم شارژ و دشارژ باتری را بر عهده دارد. این سیستم به‌طور خودکار ولتاژ و دما را کنترل می‌کند و از شارژ بیش از حد یا تخلیه بیش از حد جلوگیری می‌کند. اگر مهاجم بتواند از طریق حمله سایبری به سیستم BMS نفوذ کند، ممکن است به یکی از روش‌های زیر باتری را تخریب کند:

غیرفعال کردن مکانیسم‌های ایمنی: اگر حمله موفق شود و مهاجم دسترسی به سیستم BMS داشته باشد، می‌تواند ویژگی‌های ایمنی مانند محدودیت شارژ، محدودیت دما یا پروتکل‌های قطع شارژ را غیرفعال کند. در این حالت، باتری می‌تواند بیش از حد شارژ شود و دمای آن به شدت افزایش یابد، که در نهایت منجر به تخریب یا انفجار می‌شود.

دستکاری در الگوریتم‌های شارژ: مهاجم می‌تواند الگوریتم‌های کنترل ولتاژ و جریان شارژ را تغییر داده و اجازه دهد باتری به سرعت و با ولتاژ بالا شارژ شود که منجر به افزایش دما و فشار داخلی باتری می‌شود.

تولید گرمای بیش از حد از طریق مصرف مداوم انرژی

در برخی موارد، مهاجم می‌تواند با ایجاد حملاتی که باعث شود پردازنده دستگاه یا بخش‌های دیگر سیستم به صورت مداوم کار کنند، مصرف انرژی را به شدت افزایش دهد. این می‌تواند باتری را مجبور کند به‌طور مداوم انرژی بیشتری تولید کند و باعث شود باتری بیش از حد داغ شود. افزایش دما می‌تواند باعث تورم، نشت مواد شیمیایی و حتی انفجار باتری لیتیومی شود.

حمله به مدارهای الکتریکی

در صورتی که مهاجم بتواند از طریق نفوذ به نرم‌افزار یا سخت‌افزار پیجر، دسترسی به مدارهای الکتریکی را تغییر دهد، ممکن است با ارسال فرمان‌های غیرعادی به سیستم شارژ یا استفاده از روش‌های حمله به مدارهای الکترونیکی، موجب شارژ نادرست یا مصرف بیش از حد شود.

الف) چند نمونه از سناریوهای بالقوه برای حمله سایبری به باتری

سناریوی ۱: حمله به نرم‌افزار کنترل شارژ: مهاجم با استفاده از یک آسیب‌پذیری در نرم‌افزار پیجر، سیستم کنترل شارژ باتری را دستکاری می‌کند و به باتری اجازه می‌دهد بدون محدودیت شارژ شود. این منجر به افزایش دما و در نهایت انفجار باتری می‌شود.

سناریوی ۲: حمله افزایش دما از طریق مصرف بیش از حد انرژی: مهاجم از طریق یک بدافزار یا کد مخرب، پردازنده پیجر را وادار به انجام عملیات‌های محاسباتی سنگین به صورت مداوم می‌کند که باعث افزایش دما می‌شود. گرمای بیش از حد به باتری انتقال یافته و ممکن است به انفجار یا نشت منجر شود.

سناریوی ۳: حمله دستکاری ولتاژ: در این سناریو، مهاجم با دسترسی به مدارهای مدیریت انرژی یا از طریق نفوذ به نرم‌افزار پیجر، ولتاژ شارژ یا دشارژ باتری را به شدت افزایش می‌دهد که باعث خرابی باتری و انفجار می‌شود.

ب) راهکارهای جلوگیری از حملات سایبری به باتری‌ها

سیستم‌های حفاظت سخت‌افزاری: اطمینان از اینکه سیستم‌های مدیریت باتری (BMS) به درستی عمل می‌کنند و از شارژ بیش از حد یا دشارژ کامل جلوگیری می‌کنند.

رمزنگاری و احراز هویت قوی: استفاده از مکانیزم‌های رمزنگاری برای جلوگیری از دسترسی غیرمجاز به سیستم‌های مدیریت انرژی و شارژ.

بروزرسانی مداوم نرم‌افزارها: بروزرسانی مداوم سیستم‌های نرم‌افزاری پیجرها برای رفع آسیب‌پذیری‌های امنیتی.

استفاده از مکانیزم‌های نظارتی: استفاده از نرم‌افزارهایی که مصرف انرژی و دمای دستگاه را در زمان واقعی نظارت می‌کنند و در صورت بروز ناهنجاری‌ها هشدار می‌دهند.

توصیه‌های مدیریتی برای افزایش امنیت شبکه پیجرها

پس از خرید پیجرها، به‌ویژه در کاربردهای حساس، کنترل‌ها و رویه‌های امنیتی جامع و استانداردها و Best Practiceها باید پیاده‌سازی شوند تا از وقوع سناریوهای احتمالی حملات سایبری یا تهدیدهای ناشی از همکاری سازنده با سازمان‌های مخرب جلوگیری شود. در ادامه مهم‌ترین رویه‌ها و کنترل‌های امنیتی که باید اجرا شوند، آورده شده است:

الف) بازرسی و ممیزی امنیتی مستقل[۱۳]

بعد از خرید، لازم است یک تیم امنیتی مستقل دستگاه‌ها را از نظر سخت‌افزار و نرم‌افزار بررسی کند. این تیم باید به دنبال هرگونه درهای پشتی (backdoors)، کدهای مخرب، یا تجهیزات مخفی باشد که ممکن است برای دسترسی به سیستم یا باتری استفاده شوند. اقدامات پیشنهادی در این بازرسی شامل اجرای یک بررسی کامل سخت‌افزاری و نرم‌افزاری توسط تیم امنیتی مستقل، و بررسی کدها و نرم‌افزارهای دستگاه برای اطمینان از نبود بدافزار یا کدهای مشکوک است.

ب) کنترل‌های سخت‌افزاری[۱۴]

دستگاه‌های پیجر باید به‌طور دقیق از نظر سخت‌افزاری کنترل شوند تا از تغییرات مخفیانه یا افزودن قطعات اضافی مانند ماژول‌های رادیویی مشکوک، تراشه‌های جاسوسی یا سیستم‌های مخفی جمع‌آوری داده‌ها جلوگیری شود. اقدامات پیشنهادی در این بازرسی شامل استفاده از سیستم‌های تشخیص سخت‌افزار برای شناسایی و بررسی تمامی قطعات سخت‌افزاری، انجام اسکن فیزیکی و الکترونیکی برای شناسایی هرگونه قطعات مشکوک یا غیرضروری است.

ج) کنترل و مانیتورینگ نرم‌افزار[۱۵]

نرم‌افزار پیجرها باید بررسی و کنترل شود تا هیچ کد غیرمجاز یا بدافزاری وجود نداشته باشد. همچنین باید از به‌روزرسانی‌های امن و معتبر اطمینان حاصل شود. توصیه‌های استانداردها در این گام بررسی و تحلیل نرم‌افزار دستگاه برای اطمینان از امنیت و عدم وجود backdoor، کنترل احراز هویت برای به‌روزرسانی‌ها و فقط دریافت آپدیت‌ها از منابع رسمی و امن، استفاده از سیستم‌های ضدبدافزار و نظارت بر فعالیت‌های غیرعادی نرم‌افزار ضروری است.

د) رمزنگاری و امنیت ارتباطات[۱۶]

اطمینان از اینکه تمامی ارتباطات پیجرها از طریق رمزنگاری قوی انجام می‌شود، تا در برابر حملات استراق سمع و دستکاری پیام مقاوم باشند. برای این منظور اقداماتی مانند پیاده‌سازی الگوریتم‌های رمزنگاری قوی برای تمامی ارتباطات و پیام‌ها، استفاده از احراز هویت دوجانبه برای ارسال و دریافت پیام‌ها، و استفاده از امضاهای دیجیتال برای اطمینان از صحت و سلامت پیام‌ها توصیه می‌شود.

ه) کنترل دسترسی[۱۷]

سیستم‌های پیجر باید با استفاده از کنترل‌های دسترسی قوی محافظت شوند تا فقط کاربران مجاز بتوانند به تنظیمات دستگاه دسترسی داشته باشند. لذا، توصیه می‌شود با اقداماتی مانند پیاده‌سازی کنترل‌های دسترسی مبتنی بر نقش (RBAC) برای محدود کردن دسترسی به کاربران مجاز، استفاده از احراز هویت چندعاملی (MFA) برای ورود به سیستم‌های مدیریتی پیجرها، و استفاده از لاگ‌های امنیتی برای بررسی دسترسی‌ها و فعالیت‌های انجام‌شده در سیستم، دسترسی مجاز به سیستم‌ها را کنترل نمود.

و) کنترل‌های فیزیکی[۱۸]

پیجرها و تجهیزات مربوطه باید تحت حفاظت فیزیکی قرار گیرند تا از دسترسی فیزیکی غیرمجاز و تغییرات سخت‌افزاری توسط مهاجمان جلوگیری شود. اقداماتی مانند نگهداری پیجرها در محیط‌های ایمن و کنترل‌شده، استفاده از پلمب‌های امنیتی برای اطمینان از اینکه هیچ‌کس به‌طور فیزیکی به دستگاه‌ها دسترسی نداشته باشد مانیتورینگ دستگاه‌ها با استفاده از سایر سیستم‌های امنیتی می‌تواند در کنترل فیزیکی مورد استفاده قرار گیرد.

ز) آزمایش‌های دوره‌ای تست نفوذ[۱۹]

پیجرها باید به‌طور منظم تحت آزمایش‌های امنیتی و تست نفوذ قرار گیرند تا از ایمن بودن در برابر حملات جدید اطمینان حاصل شود. برای این منظور اقداماتی مانند انجام تست‌های نفوذ منظم توسط تیم‌های امنیتی تخصصی برای شناسایی آسیب‌پذیری‌های جدید، و بررسی دوره‌ای عملکرد سیستم مدیریت باتری (BMS) و سایر قطعات حساس ضروری است.

ح) کنترل‌های شبکه و نظارت مداوم[۲۰]

در صورتی که پیجرها به شبکه‌های ارتباطی متصل باشند، لازم است که شبکه و ترافیک آن به‌طور مداوم نظارت شود تا از هرگونه فعالیت مشکوک یا تلاش برای حمله جلوگیری شود. استفاده از سیستم‌های مانیتورینگ شبکه برای شناسایی فعالیت‌های غیرعادی یا تلاش‌های نفوذ، پیاده‌سازی فایروال‌های سخت‌افزاری و نرم‌افزاری برای محافظت از شبکه ارتباطی پیجرها، و استفاده از سیستم‌های تشخیص و جلوگیری از نفوذ ویژه پیجرها (IDS/IPS) برای شناسایی و مسدود کردن حملات احتمالی اقداماتی است که برای کنترل شبکه و نظارت مداوم توصیه می‌گردد.

ط) آموزش کارکنان و کاربران[۲۱]

کاربران پیجرها باید آموزش‌های لازم را در زمینه امنیت سایبری دریافت کنند تا از خطرات مهندسی اجتماعی و دیگر حملات آگاه باشند. اقداماتی مانند برگزاری دوره‌های آموزشی امنیت سایبری برای کارکنان و کاربران پیجرها، افزایش آگاهی در مورد تهدیدات مهندسی اجتماعی و حملات فیشینگ، و ارائه دستورالعمل‌های دقیق برای استفاده ایمن از پیجرها و پاسخ به رخدادهای امنیتی می‌تواند در آگاهی‌بخشی کارکنان و کاربران بسیار مؤثر باشد.

ی) قراردادها و الزامات حقوقی[۲۲]

قبل از خرید پیجرها، قراردادهای دقیق حقوقی باید با سازنده منعقد شود که شامل تضمین‌هایی در زمینه امنیت، شفافیت در کد و سخت‌افزار و همچنین مطابقت با استانداردهای امنیتی باشد. برای این منظور اقداماتی مانند بررسی و انعقاد قراردادهای قانونی دقیق با سازنده برای تضمین امنیت و کیفیت محصولات، استفاده از استانداردهای بین‌المللی مانند ISO/IEC ۲۷۰۰۱ برای مدیریت امنیت اطلاعات، و الزام سازنده به ارائه به‌روزرسانی‌های امنیتی منظم ضروری به‌نظر می‌رسد.

حملات سایبری به سیستم‌های پیجر، به‌ویژه در کاربردهای نظامی، می‌توانند به شکل‌های مختلفی انجام شوند. این حملات شامل شنود، دستکاری پیام، منع سرویس، و حملات جمر فرکانس هستند. استفاده از تکنیک‌های پیشرفته رمزنگاری، احراز هویت و حفاظت از فرکانس‌های رادیویی می‌تواند به شکل مؤثری جلوی این نوع حملات را بگیرد

نتیجه‌گیری

دولت‌های موفق در زمینه امنیت سایبری، چارچوب‌های قانونی و مقررات جامعی را برای مقابله با تهدیدات سایبری تدوین کرده‌اند. این کشورها از رویکردهای چندجانبه شامل قوانین سخت‌گیرانه، آموزش و آگاهی عمومی، همکاری‌های بین‌المللی و سرمایه‌گذاری در زیرساخت‌های امنیتی بهره برده‌اند تا از زیرساخت‌ها و داده‌های حساس خود در برابر تهدیدات حفاظت کنند.

پیجرهای نظامی به دلیل سادگی، اطمینان و امنیت بالا، یکی از ابزارهای حیاتی برای برقراری ارتباطات سریع و مطمئن در عملیات‌های نظامی هستند. این دستگاه‌ها با استفاده از فرکانس‌های رادیویی امن و سیستم‌های رمزنگاری پیشرفته، به نیروهای نظامی امکان می‌دهند تا در هر شرایطی پیام‌ها و اطلاعات حیاتی را با کمترین تأخیر ارسال و دریافت کنند. حمله سایبری اخیر رژیم صهیونیستی بر روی پیجرها و دستگاه‌های بی‌سیم حزب‌الله در لبنان نشان داد که فراتر از تجهیزات مبتنی بر IP، حتی تجهیزاتی که از طریق فرکانس‌های رادیویی خاص و امن استفاده می‌کنند نیز می‌توانند هدف حمله قرار گیرد و هزینه‌های جبران‌ناپذیری را به دولت‌ها تحمیل نماید.

حملات سایبری به سیستم‌های پیجر، به‌ویژه در کاربردهای نظامی، می‌توانند به شکل‌های مختلفی انجام شوند. این حملات شامل شنود، دستکاری پیام، منع سرویس، و حملات جمر فرکانس هستند. استفاده از تکنیک‌های پیشرفته رمزنگاری، احراز هویت و حفاظت از فرکانس‌های رادیویی می‌تواند به شکل مؤثری جلوی این نوع حملات را بگیرد. افزایش آگاهی کاربران و پیاده‌سازی راهکارهای امنیتی مدرن می‌تواند مقاومت سیستم‌های پیجر در برابر حملات سایبری را به طور قابل توجهی افزایش دهد.

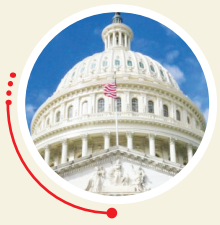
در حالی که امکان تئوری حمله سایبری به باتری‌های لیتیوم برای انفجار آن‌ها وجود دارد، اجرای موفقیت‌آمیز این حملات نیازمند دسترسی عمیق به سیستم‌های سخت‌افزاری و نرم‌افزاری است. سیستم‌های حفاظتی موجود معمولاً از وقوع چنین حملاتی جلوگیری می‌کند، اما با توجه به پیشرفت فناوری و کشف آسیب‌پذیری‌های جدید، همیشه باید آمادگی لازم برای مقابله با حملات احتمالی وجود داشته باشد. رعایت الزامات و رویه‌های کنترلی استاندارد می‌تواند امکان چنین حملاتی را به حداقل برساند.

پی‌نوشت‌ها:

1- Eavesdropping
2- frequency hopping
3- Message Tampering
4- Denial of Service (DoS)
5- Radio Frequency Jamming
6- spread spectrum
7- Replay Attack
8- Frequency Hijacking
9- Interference Attack
10- Spoofing
11- Social Engineering
12- Battery Management System
13- Security Audit
14- Hardware Controls
15- Software Control & Monitoring
16- Encryption & Secure Communication
17- Access Control
18- Physical Security Controls
19- Regular Testing & Penetration Testing
20- Network Controls & Continuous Monitoring
21- Training & Awareness
22- Legal Agreements & Compliance

تاخیر یا لغو سفر نتانیاهو به آمریکا

رسانه‌های رژیم اسرائیل از بسته شدن حریم هوایی مناطقی از شمال فلسطین از شهر الخضیره در جنوب حیفا تا مرزهای لبنان خبر دادند. رسانه‌ها دلیل بسته شدن آسمان این منطقه را اوضاع متشنج و احتمال حملات تلافی‌جویانه حزب‌الله لبنان اعلام کرده‌اند. نماینده اسرائیل در سازمان ملل متحد نیز گفت که بنیامین نتانیاهو نخست‌وزیر این رژیم، سفر برنامه‌ریزی‌شده خود به آمریکا را کوتاه و یا لغو خواهد کرد. دنی دنن در گفت‌وگو با خبرنگاران در مقر سازمان ملل متحد در نیویورک اعلام کرد که این سفر به تاخیر افتاده و تحولات داخلی در رژیم صهیونیستی ممکن است برنامه سفر نتانیاهو را تحت تأثیر قرار دهد. پیش‌تر روزنامه عبری‌زبان اسرائیل الیوم اعلام کرده بود که نتانیاهو سفر هفته آینده خود به نیویورک برای شرکت در نشست مجمع عمومی سازمان ملل متحد را به سبب تشدید تنش در مرزهای شمالی کوتاه خواهد کرد و سفر او یک روزه خواهد بود.



آغاز رای‌گیری زودهنگام انتخابات آمریکا

هفت هفته مانده به انتخابات ریاست‌جمهوری آمریکا، در سه ایالت این کشور، رأی‌گیری پیش از موعد برای انتخابات ریاست‌جمهوری ۲۰۲۴ آمریکا برگزار شد. رأی‌دهندگان در ایالات مینه‌سوتا، داکوتای جنوبی و ویرجینیا رأی خود را به صندوق انداختند. بیش از ۱۰ ایالات دیگر آمریکا نیز اواسط ماه آینده (اواسط اکتبر) و پیش از برگزاری انتخابات ریاست‌جمهوری در ماه نوامبر، رأی خواهند داد. آغاز رأی‌گیری حضوری در پی یک تابستان آشفته در سیاست آمریکا صورت گرفته که شامل رخدادهایی چون کناره‌گیری جو بایدن از دور رقابت‌های انتخاباتی و جایگزین شدن هریس به جای او و طرح ترور دونالد ترامپ می‌شود. گزارش‌ها حاکی از آن است که علاوه بر رأی‌گیری حضوری امکان انداختن آراء به صندوق‌های پستی نیز در سه ایالت مذکور وجود داشت. بسیاری از رأی‌دهندگانی که روز گذشته در انتخابات زودهنگام شرکت کردند، ابراز نگرانی کردند که احتمال می‌دهند که در روز انتخابات شاهد هرج و مرج باشند و به همین دلیل ترجیح دادند زودتر در انتخابات شرکت کنند.

تجارت پنهانی سراسر اروپا با روسیه

پیتر سیجارتو، وزیر خارجه مجارستان با بیان اینکه بوداپست باید همکاری خود به‌ویژه در حوزه اقتصادی را با مسکو حفظ کند، تاکید کرد: «تمام اروپا به طور پنهانی با روسیه تجارت می‌کنند.» سیجارتو با اشاره به لزوم تداوم نشست کمیسیون بین دولتی همکاری اقتصادی روسیه و مجارستان (IGC)، در پیامی در حساب کاربری خود در رسانه اجتماعی ایکس (توئیتر سابق) نوشت: «بوداپست نیاز به توسعه همکاری با مسکو دارد چراکه این امر منافع ملی مجارستان و مردم این کشور را تامین می‌کند.» وزیر خارجه مجارستان در ادامه با بیان اینکه بوداپست علاقه‌مند به توسعه همکاری بین مجارستان و روسیه در حوزه‌هایی است که تحت تحریم‌های اتحادیه اروپا قرار نگرفته است، خاطرنشان کرد: «به هر حال، تمام اروپا با روس‌ها تجارت می‌کنند اما تفاوت آنها با ما این است که آنها سعی می‌کنند این موضوع را پنهان کنند.» پاول ماریشف، عضو شورای تخصصی در انجمن گاز روسیه پیش‌تر با اشاره به اینکه روسیه چهارمین صادرکننده بزرگ گاز ال‌ان‌جی (LNG) در دنیا است، اظهار کرد: «اتحادیه اروپا همچنان بزرگترین مشتری گاز روسیه است.»