وزارت ارتباطات و فناوری اطلاعات
پژوهشگاه ارتباطات و فناوری اطلاعات

معرفی نمونه‌های واقعی از نقض امنیت سایبری توسط نهادها، شرکت ها و محصولات کشور آلمان

عنوان گزارش: معرفی نمونه‌های واقعی از نقض امنیت سایبری توسط نهادها، شرکت‌ها و محصولات کشور آلمان

کلمات کلیدی: امنیت سایبری، شنود، بدافزار و کشور آلمان

تهیه کننده: مجید رسولی‌دیسفانی

ناظر علمی: امیرمنصور یادگاری

گروه پژوهشی: ارزیابی امنیت شبکه وسامانه‌ها

۱۴۰۴

چکیده

کشور آلمان یکی از کشورهای پیشرو در ارائه محصولات و خدمات در حوزه فاوا و امنیت سایبری در سطح بین المللی می باشد. در این گزارش سعی شده است تا بر اساس اخبار و اطلاعات منتشر شده، نمونه های واقعی از نقض امنیت سایبری توسط دولت و شرکت های آلمانی، شرکت های مهم و قوانین کلیدی پشتیبان در کشور آلمان مورد بررسی قرار گیرد. بررسی های انجام شده نشان می دهد که موارد نقض امنیت سایبری محدود به شبکه های مخابراتی نبوده و موارد متعددی در بخش های صنعتی، زیرساخت های مخابراتی، نظارت شهری، محصولات مصرف کننده، برنامه های کاربردی و بدافزارهای دولتی و رمزنگاری توسط دولت و شرکت های آلمان تا کنون ثبت شده است. از جمله موارد مهم می توان به تروجان دولتی (با پشتیبانی قانونی) برای شنود و رصد افراد و همچنین همکاری بلندمدت بین نهادهای امنیتی و اطلاعاتی آلمان با کشور ایالات متحده در زمینه شنود شبکه های مخابراتی و دستگاه های تلفن همراه مبتنی بر تجهیزات و محصولات مختلف اشاره کرد. این نقض امنیت سایبری طیف وسیعی از کشورها را دربرمی گیرد که از جمله آنها می توان به بدافزار معروف استاکس‌نت(Stuxnet) به عنوان یک ضعف مهم در نرم‌افزار نظارت صنعتی شرکت زیمنس اشاره کرد که کشورمان را تحت تاثیر قرار داد.

فهرست مطالب

۱ مقدمه

این سند با هدف بررسی نمونه های نقض امنیت سایبری توسط شرکت ها و موسسات کشور آلمان مبتنی بر گزارش ها و اخبار افشا شده تهیه شده است. بر این اساس ابتدا به بررسی نمونه های واقعی از نقض امنیت سایبری می پردازیم. سپس نمونه هایی از شرکت شرکت های مهم مطرح کشور آلمان در ارائه تجهیزات نظارتی زیرساخت و خدمات حوزه فاوا و قوانین مرتبط پشتیبان در این کشور آورده شده است. بر اساس بررسی های انجام شده، روش های متعددی برای دسترسی مخفیانه به اطلاعات و کنترل از راه دور در حوزه های صنعتی، زیرساخت های ارتباطی، برنامه های کاربردی و محصولات نهایی سمت کاربر مبتنی بر خلاء های امنیتی و یا تعبیه ویژگی های پنهان سخت افزاری و نرم افزاری مورد استفاده قرار گرفته است. نمونه های واقعی بررسی شده نشان می دهد که نقض امنیت سایبری در بسیاری از کشورها و در مواردی با همکاری نهادهای اطلاعاتی و امنیتی صورت پذیرفته است. از جمله مواردی که کشورمان را تحت تاثیر قرارد داد، می توان به بدافزار معروف استاکس‌نت (Stuxnet) به عنوان یک ضعف مهم در نرم‌افزار نظارت صنعتی شرکت زیمنس اشاره کرد.

۲ نمونه های واقعی نقض امنیت سایبری توسط شرکت‌های آلمانی

در دهه‌ی گذشته موارد متعددی افشا شده که نشان می‌دهد برخی شرکت‌های آلمانی یا شرکت‌هایی با مرکز توسعه در آلمان، به‌طور عمدی قابلیت‌های مخفی در محصولات سخت‌افزاری یا نرم‌افزاری خود تعبیه کرده‌اند که بدون اطلاع کاربر به جمع‌آوری، انتقال یا پردازش اطلاعات می‌پردازند. این روش‌ها فراتر از مفهوم متداول درب پشتی (Backdoor) هستند و شامل طیفی از ترفندهای پنهانی می‌شوند که امنیت سایبری را نقض کرده یا حریم خصوصی و اطلاعات کاربران را در معرض سوءاستفاده قرار داده‌اند. در این بخش مصادیق واقعی از نمونه های نقض امنیت سایبری بر أساس موارد افشا شده ارائه می شود.

۱) روش‌های تعبیه‌شده‌ی عمدی در محصولات برای دسترسی مخفیانه به اطلاعات

منظور از روش‌های تعبیه‌شده‌ی عمدی، قابلیت‌هایی پنهان یا آسیب‌پذیری‌های عامدانه در سامانه‌هاست که به سازندگان یا اشخاص ثالث امکان دسترسی غیرمجاز به داده‌ها یا کنترل از راه دور سیستم را می‌دهد؛ بدون آن‌که بهره‌بردار (کاربر یا سازمان خریدار) از وجود آن‌ها مطلع باشد. این روش‌ها می‌توانند شامل موارد زیر باشند:

- **درهای پشتی غیراستاندارد:** حساب‌های کاربری یا کلمات‌عبور پیش‌فرض پنهان، یا دستورات و پروتکل‌های undocumented که به دسترسی سطح بالا منجر می‌شوند.
- **ویژگی‌های پنهان سخت‌افزاری:** مدارها، ماژول‌ها یا مودهای مخفی در سخت‌افزار که امکان استخراج داده یا کنترل سیستم را فراهم می‌کنند.
- **بدافزارهای تعمدی در نرم‌افزار:** کدهای مخربی که عمداً توسط توسعه‌دهنده در نرم‌افزار یا firmwareگنجانده شده و به جمع‌آوری یا انتقال اطلاعات کاربران می‌پردازد.
- **استفاده سوء از قابلیت‌های قانونی:** برخی محصولات برای مقاصد قانونی نظیر*شنود قانونی* طراحی می‌شوند، اما می‌توانند مخفیانه و فراتر از محدوده‌ی تعریف‌شده استفاده شوند.

۲) نمونه‌های نقض امنیت سایبری در حوزه صنعتی (سامانه‌های کنترل صنعتی و محصولات زیرساختی)

- **قابلیت دسترسی مخفی درPLC های زیمنس:** در سال ۲۰۱۹ پژوهشگران دانشگاه-Ruhr Bochumآلمان کشف کردند که در کنترل‌کننده‌های منطقی قابل‌برنامه‌ریزی سری-SIMATIC S7 1200شرکت زیمنس، یک حالت دسترسی سخت‌افزاری مستندنشده وجود دارد. این قابلیت که احتمالاً برای تشخیص عیب در کارخانه تعبیه شده بود، به صورت مخفی در bootloader سخت‌افزار فعال است. مهاجم با دسترسی فیزیکی و ارسال فرمان خاص از طریق رابط UART در نیم‌ثانیه‌ی اول بوت شدن دستگاه، می‌تواند این حالت ویژه دسترسی را فعال کند. نتیجه سوءاستفاده از این در پشتی سخت‌افزاری آن است که مهاجم قادر خواهد بود حافظه‌ی PLC را تخلیه کرده و حتی کد دلخواه را در مرحله‌ی Bootloaderاجرا کند. [1]
- **زیمنس (نرم‌افزار WinCC/PCS7 با** کلمه‌عبور ثابت **در پایگاه‌داده SCADA):** در سال ۲۰۱۰ و در جریان کشف بدافزار معروف استاکس‌نت(Stuxnet) ، یک ضعف مهم در نرم‌افزار نظارت صنعتی (*Siemens SIMATIC WinCC* بخشی از سکوی SCADA شرکت زیمنس فاش شد. مشخص گردید

[1] https://itwire.com/business-it-news/security/researchers-find-backdoor-in-siemens-plcs.html#:~:text=S7,to%20violate%20the%20existing%20security

که WinCC و سامانه کنترل فرایند PCS7 از یک کلمه‌عبور ثابت و از پیش تعریف‌شده برای اتصال به پایگاه‌داده خود استفاده می‌کنندمهاجمان استاکس‌نت با سواستفاده از همین درب‌پشتی توانستند به پایگاه‌داده پروژه‌های صنعتی دسترسی یافته و بدافزار خود را در سیستم‌های کنترل غنی‌سازی اورانیوم در ایران تزریق و اجرا کنند. در واقع، WinCCدارای حساب پیش‌فرض پایگاه‌داده بود که بدون اطلاع مدیران سیستم و بدون امکان تغییر مؤثر، در نرم‌افزار تعبیه شده بود. [1]

- **درب‌پشتی در نرم‌افزار CoDeSys کنترل‌گرهای صنعتی:** شرکت آلمانی *Smart Software Solutions* سازنده نرم‌افزار CoDeSys است که یک پلتفرم برنامه‌نویسی PLC طبق استاندارد IEC 61131-3می‌باشد. در سال ۲۰۱۲ مشخص شد نسخه‌هایی از CoDeSys یک درب‌پشتی تعبیه‌شده دارد: مهاجم می‌تواند بدون هیچ‌گونه احراز هویت از طریق شبکه به کنترل‌گرهای صنعتی مبتنی بر CoDeSys متصل شود و فرمان اجرا کند. این نرم‌افزار در تجهیزات بیش از ۲۵۰ تولیدکننده صنایع مختلف (نظیر انرژی، نظامی و دریانوردی) به‌کار رفته و هزاران کاربر صنعتی از آن بهره می‌گیرند. آسیب‌پذیری به این صورت است که CoDeSys دارای یک *رابط خط فرمان* مخفی روی پورت TCP 1200 است که حتی در صورت تنظیم گذرواژه برای رابط گرافیکی، همچنان آزاد و بدون کلمه‌عبور در دسترس می‌ماند. در این حالت مهاجم قادر است از راه دور کل منطق برنامه‌ی PLC را مشاهده، متوقف یا پاک کند و حتی با قراردادن گذرواژه، دسترسی اپراتور قانونی را قفل نماید. [2]
- **نمونه‌ی پرابهام نقص رمزنگاری(Infineon)** : در سال ۲۰۱۷ مشخص شد که الگوریتم تولید کلید RSAدر تراشه‌های امن شرکت آلمانی اینفینیون (Infineon) دارای یک ضعف بنیادین است که به مهاجم اجازه می‌دهد از روی کلید عمومی، کلید خصوصی را محاسبه کند. این رخنه‌ی موسوم به ROCA میلیون‌ها کارت هوشمند، توکن امنیتی و حتی مدارک هویتی الکترونیک را تحت‌الشعاع قرار داد. هرچند تحقیقات مستقل هیچ *شواهدی از عمدی بودن* این ضعف ارائه نکرده و احتمالاً یک خطای برنامه‌نویسی بوده است، اما وسعت و ماهیت آسیب‌پذیری برخی کارشناسان را نسبت به امکان تعبیه عمدی نقاط ضعف رمزنگاری در محصولات سخت‌افزاری به تردید واداشت. در هر حال، این مورد اهمیت *بازبینی دقیق مستقل* محصولات صنعتی–امنیتی را نشان داد. [3]

۳) نمونه های نقض امنیت سایبری در حوزه مخابراتی (شبکه‌ها و تجهیزات شنود در مخابرات)

صنایع مخابراتی آلمان نیز در مواردی با اتهام مشارکت در نقض پنهانی امنیت ارتباطات روبرو بوده‌اند. این موارد عمدتاً به تجهیزاتی برمی‌گردد که به دولت‌ها امکان شنود و پایش مخفیانه‌ی ارتباطات مخابراتی را می‌دهد. فروش فناوری‌های شنود و صادرات این فناوری ها طبق قوانین کنترل صادرات آلمان (مصادیق دو کاربرده) قرار دارد.

- **فروش سامانه‌های شنود توسط شرکت Trovicor** : این شرکت یکی از تولیدکنندگان اصلی

---

[1] https://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=SCADA#:~:text=CVE,2568, https://www.trendmicro.com/vinfo/br/threat-encyclopedia/web-attack/54/stuxnet-malware-targets-scada-systems#:~:text=Default%20Password%20Security%20Bypass%20Vulnerability,information%20can%20be%20found%20below

[2] https://www.heise.de/news/Steuerungssysteme-mit-Hintertuer-1738466.html#:~:text=Die%20Programmiersoftware%20CoDeSys%20des%20deutschen,Berater%20bei%20digital%20bond

[3] https://arstechnica.com/information-technology/2017/10/crypto-failure-cripples-millions-of-high-security-keys-750k-estonian-ids/#:~:text=Millions%20of%20high,stakes%20settings

"Monitoring Center" یا مراکز نظارت مخابراتی است. این سامانه‌ها می‌توانند به شبکه‌های مخابراتی متصل شده و به‌طور گسترده مکالمات تلفنی، پیامک‌ها و حتی ترافیک اینترنتی را به‌صورت مخفی شنود و ضبط کنند. اگرچه این محصولات رسماً فقط به نهادهای دولتی فروخته می‌شوند و تحت عنوان *شنود قانونی* عرضه می‌گردند، مواردی از فروش این محصولات به نهادهای غیردولتی در برخی کشورها گزارش شده است.

- بنا بر گزارش های منتشر شده، در بحرین، نرم‌افزار Monitoring Center شرکت Trovicor نقش مستقیم در شناسایی و دستگیری فعالان حقوق بشری داشته است. همچنین رسانه های آلمانی گزارش هایی از فروش این نمونه سامانه ها به نهادهای غیردولتی در ایران پیش از سال ۲۰۰۹ منتشر شده است. رسانه‌های آلمانی نیز فاش کردند که در بحبوحه جنگ داخلی سوریه (۲۰۱۱–۲۰۱۲)، رژیم سوریه به سامانه‌های شنود سایبری پیشرفته‌ای دست یافته که گمان می‌رود یکی از تامین‌کنندگان آن‌ها Trovicor بوده است. [1]

- **همکاری سرویس اطلاعات فدرال آلمان و آژانس امنیت ملی آمریکا در شنود فراگیر:** ماجرای همکاری مخفیانه BND با آژانس امنیت ملی آمریکا (NSA) هرچند مستقیماً به یک محصول فروخته‌شده مرتبط نبود، اما مستلزم دسترسی پنهانی به شبکه‌های شرکت‌های مخابراتی آلمان بود. در عملیات مشترکی موسوم به *ایکونال (Eikonal)* ، سرویس اطلاعات فدرال آلمان (BND) با همکاری دویچه تلکوم یک شبکه فیبرنوری در فرانکفورت را به طور مخفی شنود می‌کرد و داده‌ها را در اختیارآژانس امنیت ملی امریکا NSA می‌گذاشت. این اقدام در سال ۲۰۱۴ افشا شد و به یک رسوایی سیاسی انجامید. [2]

۴) نمونه های نقض امنیت سایبری در حوزه شهری و انتظامی (نظارت شهری و ابزارهای پلیسی)

- **دستگاه‌های IMSI-Catcher ساخت آلمان:** یکی از شناخته‌شده‌ترین ابزارهای نظارتی پلیس در شهرها، آی‌ام‌اس‌آی–کچر (IMSI-Catcher) است. این دستگاه که نخستین نمونه‌های آن در اواسط دهه ۹۰ میلادی توسط شرکت Rohde & Schwarz آلمان ساخته شد. عملاً یک دکل مخابراتی جعلی قابل‌حمل است. این دستگاه با شبیه‌سازی یک برج مخابراتی، همه تلفن‌های همراه اطراف را وادار به اتصال به خود می‌کند و بدین طریق شناسه‌های مشترکین (IMSI) و سایر اطلاعات آن‌ها را استخراج می‌کند. این دستگاه قادر است مکالمت و پیامک‌ها را شنود کند؛ زیرا پس از فریب گوشی و قرار دادن آن در حالت ناامن (غیررمزشده)، می‌تواند گفتگوها را ضبط و حتی با انجام حمله مرد *میانی* آن‌ها را رهگیری نماید.کاربران تلفن همراه هیچ نشانه‌ای از این شنود دریافت نمی‌کنند و ممکن است ساعت‌ها ارتباطاتشان

---

[1] https://de.wikipedia.org/wiki/Trovicor#:~:text=Das%20Unternehmen%20wurde%201993%20urspr%C3%BCnglich,5, http://www.zdnet.de/news/wirtschaft_unternehmen_business_nokia_siemens_bestreitet_lieferung_von_abhoertechnik_an_iran_story-39001020-41005652-1.htm, https://web.archive.org/web/20090831070713/http://www.perusa-partners.de/deutsch/beteiligungen/beteiligungen.php

[2] https://www.zeit.de/politik/ausland/2020-02/bnd-cia-geheimdienste-verschluesselte-kommunikation-zdf#:~:text=2,Stellungnahme%20vom%20BND

زیر نظر باشد. در آلمان استفاده از IMSI-Catcher توسط پلیس و سرویس‌های اطلاعاتی از سال ۲۰۰۲ به‌طور قانونی مجاز شده است، اما تنها با مجوز قضایی. با این حال، مواردی گزارش شده که از این دستگاه برای پایش گسترده تجمعات و اعتراضات در شهرهای آلمان استفاده شده است. هر بار افشای چنین عملکردی موجب نگرانی فعالان حقوق مدنی شده؛ چرا که این دستگاه برای ردیابی یک مظنون، داده تمامی شهروندان حاضر در محدوده را نیز جمع‌آوری می‌کند –که نقض آشکار اصل تناسب و حریم خصوصی است. [۱]

- **سامانه‌های نظارت تصویری و تشخیص چهره:** شرکت‌های آلمانی در حوزه‌ی سامانه‌های دوربین مدار بسته و نرم‌افزارهای تحلیلی نقش دارند. مثلاً شرکت‌هایی نظیر Bosch و Siemens بخش‌هایی در زمینه‌ی *شهر هوشمند* و نظارت شهری دارند. هرچند تا کنون موردی دال بر *تعبیه درِ پشتی* در این سامانه‌ها گزارش نشده، اما آزمایش‌های مخفی تشخیص چهره در ایستگاه‌های قطار آلمان (همچون آزمایش ایستگاه Südkreuzبرلین در سال ۲۰۱۷) بدون اطلاع قبلی عموم، زنگ خطرهایی را به صدا درآورد. در این آزمایش از ترکیب دوربین‌های شهری و نرم‌افزار هوشمند (تأمین‌شده توسط شرکت‌های خارجی و آلمانی) برای شناسایی چهره‌ی افراد استفاده شد. هرچند هدف، آزمایش توان فناوری عنوان گردید، ولی انجام آن بدون آگاهی شهروندان و عدم شفافیت در مورد دیتای جمع‌آوری‌شده، نقدهای زیادی برانگیخت. این نمونه نشان می‌دهد که حتی در حوزه‌ی شهری نیز جمع‌آوری داده‌ی مخفیانه می‌تواند توسط تجهیزات شهری صورت گیرد، هرچند به اسم ارتقای امنیت یا خدمات[۲].

۵) نمونه های نقض امنیت سایبری در حوزه محصولات مصرف‌کننده (دستگاه‌ها و نرم‌افزارهای کاربری)

- **روترهای خانگی دارای در پشتی پنهان:** در سال ۲۰۱۲ آشکار شد که سه مدل از روترهای وای‌فای Speedportمتعلق به شرکت Deutsche Telekom دارای یک حفره امنیتی عمده هستند. در این دستگاه‌ها، حتی اگر کاربر قابلیت WPS اتصال با PIN را غیرفعال می‌کرد، در عمل یک PIN پیش‌فرض ساده در firmware روتر تعبیه شده بود که همیشه فعال باقی می‌ماند. به عبارت دیگر، برخلاف آنچه در تنظیمات به کاربر نمایش داده می‌شد، شبکه‌ی Wi-Fi این روترها همواره از طریق WPS با یک رمز ثابت قابل نفوذ بود. این در پشتی عملاً به هر فرد مهاجم اجازه می‌داد بدون دانش کاربر به شبکه بی‌سیم او متصل شده، به تبادل داده‌هایش گوش کند یا از اتصال وی سوءاستفاده نماید. [۳]
- **اپلیکیشن‌ها و افزونه‌های جاسوسی:** در عرصه نرم‌افزارهای مصرفی نیز نمونه‌های مشهوری وجود دارد. برای مثال، افزونه مرورگر Web of Trust (WOT)که در ظاهر ساخت یک استارتاپ فنلاندی بود ولی توسط رسانه‌های آلمانی افشا شد که در حال فروش مخفیانه داده‌های تاریخچه مرورگری میلیون‌ها

[1] https://www.heise.de/thema/IMSI_Catcher#:~:text=IMSI,Mehr%20anzeigen

[2] https://www.reuters.com/article/world/german-police-test-facial-recognition-cameras-at-berlin-station-idUSKBN1AH4VS/?utm_source=chatgpt.com, https://edri.org/our-work/controversial-testing-of-facial-recognition-software-in-germany/?utm_source=chatgpt.com, https://www.dw.com/en/big-brother-in-berlin-face-recognition-technology-gets-tested/a-39912905?utm_source=chatgpt.com

[3] https://www.welt.de/wirtschaft/webwelt/article106232281/Speedport-Modelle-Telekom-stopft-offene-Hintertuer-in-WLAN-Router.html#:~:text=Danach%20liegt%20die%20Schwachstelle%20in,Aktivit%C3%A4ten%20missbrauchen%2C%20berichtete%20das%20Portal

کاربر به شرکت‌های ثالث است. بررسی‌ها نشان داد که WOT حجم عظیمی از اطلاعات شامل همه سایت‌های بازدیدشده به همراه جزئیاتی نظیر شناسه کاربر، آدرس ایمیل، عادات خرید، حتی سوابق بیماری یا تمایلات شخصی را جمع‌آوری کرده و به شکل ناکافی ناشناس‌سازی‌شده فروخته است. این رسوایی در سال ۲۰۱۶ توسط شبکه تلویزیونی NDR آلمان علنی شد و بلافاصله افزونه WOT از فروشگاه‌های مرورگرها حذف گردید. [۱]

- **دستگاه‌های آلوده‌شده در زنجیره تأمین:** یکی دیگر از چالش‌های امنیت مصرف‌کنندگان، آلوده شدن عمدی دستگاه‌ها در فرآیند تولید است. برای نمونه، در سال ۲۰۲۱ گزارش شد برخی گوشی‌های هوشمند برند آلمانی **Gigaset** دچار بدافزار سیستمی شده‌اند که اطلاعات کاربران را سرقت می‌کند. بررسی‌ها نشان داد سرور به‌روزرسانی نرم‌افزار این شرکت توسط عوامل ناشناس هک و یک آپدیت حاوی بدافزار به دستگاه‌ها فرستاده شده است. هرچند این مورد تقصیر مستقیم شرکت نبود و ناشی از یک حمله‌ی زنجیره تأمین بود، اما *نشانگر آسیب‌پذیری مسیرهای انتشار نرم‌افزار* است. [۲]

۶) نمونه های نقض امنیت سایبری در حوزه اپلیکیشن‌های امنیتی و نظارتی (بدافزارهای دولتی و ابزارهای رمزنگاری)

این حوزه شاید بحث‌برانگیزترین موارد نقض عمدی امنیت سایبری توسط شرکت‌های آلمانی را دربرمی‌گیرد، چرا که به ابزارهایی مربوط می‌شود که ظاهراً برای اهداف امنیتی یا مجری قانون ساخته شده‌اند اما خود نقض‌کننده امنیت و حریم خصوصی هستند.

- **تروجان دولتی ساخت آلمان (Bundestrojaner)** : در سال ۲۰۱۱ انجمن مشهوری به نام باشگاه کامپیوتر کائوس (CCC) موفق به کشف و مهندسی معکوس بدافزاری شد که در سیستم یک فرد مظنون (به دستور پلیس ایالتی) نصب شده بود. این بدافزار که بعدها با نام عام *تروجان دولتی* شناخته شد، توسط یک شرکت خصوصی آلمانی (احتمالاً DigiTaskبه قراردادی با دولت) توسعه یافته بود. طبق حکم قانونی، پلیس صرفاً مجاز بود از این ابزار برای شنود ارتباطات اینترنتی (مثلاً تماسSkype)استفاده کند اما تحلیل CCCنشان داد که تروجان مذکور فراتر از حدود مجاز عمل می‌کند: این بدافزار می‌توانست بر روی سیستم قربانی نرم‌افزار دلخواه از راه دور نصب و اجرا کند و عملاً دسترسی کامل به کل کامپیوتر (فایل‌ها، میکروفون، وب‌کم، کی‌بورد و ...) بدهد. به علاوه، به دلیل ضعف‌های فنی فاحش، هر مهاجم دیگری نیز می‌توانست کنترل بدافزار را در دست گرفته و اطلاعات جعلی تزریق کند یا سیستم را آلوده‌تر کند. این کشف یک رسوایی بزرگ در آلمان به‌پا کرد؛ زیرا اثبات شد نهادهای مجری قانون عمداً یک «درِ مخفی همه‌کاره» روی رایانه شهروندان مظنون قرار داده‌اند که نه تنها حریم خصوصی را نقض می‌کند بلکه امنیت سیستم را نیز برای سایر مهاجمان باز می‌گذارد. [۳]

---

[۱] https://thehackernews.com/2016/11/web-of-trust-addon.html#:~:text=An%20investigation%20by%20German%20television,help%20keep%20them%20safe%20online

[2] https://www.cyberdefensemagazine.com/gigaset-android/?utm_source=chatgpt.com, https://www.bleepingcomputer.com/news/security/gigaset-android-phones-infected-by-malware-via-hacked-update-server/?utm_source=chatgpt.com

[3] https://netzpolitik.org/2014/geheimes-dokument-bundeskriminalamt-darf-finfisher-finspy-nicht-einsetzen-versucht-einfach-neue-version-nochmal/#:~:text=Seit%20Januar%202013%20wissen%20wir,nicht%20vom%20Gesetz%20gedeckt%20waren ,

- **جاسوس‌افزار تجاری ساخت آلمان FinFisher/FinSpy:** یکی از جنجالی‌ترین نمونه‌ها، نرم‌افزار جاسوسی FinSpy است که توسط شرکت آلمانی-بریتانیایی FinFisher GmbH (مستقر در مونیخ) توسعه یافته است. فین‌اسپای یک بدافزار بسیار پیشرفته است که به طور انحصاری به دولت‌ها و نیروهای پلیس فروخته می‌شود و قادر است *کنترل کامل رایانه یا گوشی هوشمند هدف* را به دست گیرد. این بدافزار می‌تواند لیست مخاطبین، پیام‌های چت، مکالمات تلفنی، عکس‌ها و ویدیوهای قربانی را (حتی در برنامه‌های رمزنگاری‌شده‌ای مانند واتس‌اپ یا سیگنال) استخراج کند و به سرور مهاجم ارسال نماید. همچنین قابلیت فعال‌سازی میکروفون و دوربین دستگاه و ثبت کلیدهای فشرده‌شده (Keylogger) را دارد. نخستین بار در خلال انقلاب مصر (۲۰۱۱) چند نمونه از FinSpy در دفتر امنیتی حسنی مبارک پیدا شد که نشان می‌داد رژیم مصر از نسخه‌ای از این بدافزار برای رصد مخالفان استفاده کرده است. از آن پس تحقیقات Citizen Labو دیگران نشان داد که FinFisher/FinSpy در کشورهای متعددی از جمله بحرین، اتیوپی، میانمار و ویتنام استفاده شده است. در یک نمونه بسیار خبرساز، در جریان اعتراضات ۲۰۱۷ ترکیه (موسوم به «راهپیمایی عدالت»)، لینک‌هایی جعلی در توییتر منتشر شد که حاوی اپلیکیشن موبایلی ظاهراً برای سازماندهی تظاهرات بود. این اپلیکیشن در حقیقت نسخه‌ای از FinSpy مخصوص اندروید بود که پس از نصب، گوشی معترضان را به طور کامل تحت نظارت دولت ترکیه قرار می‌داد. تحقیقات رسانه‌ای آلمان نشان دادند که این جاسوس‌افزار توسط FinFisher به ترکیه *بدون مجوز صادرات* تحویل داده شده است. گزارش‌ها نشان داد که پلیس فدرال آلمان (BKA) نیز در ابتدا قصد خرید FinSpy را داشت و نسخه‌هایی را آزمایش کرده بود. اما به دلیل وجود قابلیت‌های غیرقانونی) مثل همان دسترسی کامل و فراتر از شنود مجاز)، استفاده از آن برای پلیس آلمان ممنوع اعلام شد. بر أساس گزارش ها، BKA توسعه تروجان بومی خود را به جای تکیه بر محصول این شرکت در پیش گرفت. [1]
- **دستکاری رمزنگاری توسط BND و مشارکت شرکت‌ها:** شاید بزرگ‌ترین افشاگری در حوزه‌ی *رمزنگاری*، ماجرای عملیات Rubikon باشد که در سال ۲۰۲۰ فاش شد. در این عملیات سری که از دهه ۱۹۷۰ آغاز شده بود، سازمان اطلاعات فدرال آلمان (BND) به همراه CIA آمریکا به طور مخفیانه مالکیت یک شرکت سوئیسی به نام Crypto AGرا در اختیار داشتند. کریپتو AG تولیدکننده دستگاه‌های رمزنگار (برای مخابرات امن) برای ده‌ها کشور بود. BND و CIA از طریق نفوذ بر این شرکت، عمداً الگوریتم‌های رمزنگاری دستگاه‌ها را تضعیف یا دارای درِ پشتی طراحی کردند. به‌طوری‌که خودشان قادر به شکستن رمز و خواندن پیام‌های به‌ظاهر محرمانه بودند. در نتیجه، طی سال‌های جنگ سرد و پس از آن، *بیش از ۱۰۰ کشور*) از جمله ایران، کشورهای عربی، آمریکای لاتین، حتی واتیکان) که تجهیزات Crypto AG را خریده بودند، عملاً تمام مکاتبات حساس خود را ناخواسته برای آلمان و آمریکا افشا می‌کردند. این همکاری تا سال ۱۹۹۳ توسط آلمان ادامه یافت (سپس BND سهام خود را واگذار کرد) اما CIA تا حدود ۲۰۱۸ همچنان از این تله استفاده می‌کرد. افشای این حقیقت در گزارش مشترک واشنگتن‌پست و تلویزیون ZDFآلمان (فوریه ۲۰۲۰) بهت و رسوایی بزرگی به بار آورد و بسیاری این اقدام را بزرگ‌ترین خیانت در

https://www.ccc.de/de/updates/2011/staatstrojaner#:~:text=Spionagesoftware%20vorgenommen,die%20auch%20Dritte%20ausnutzen%20k%C3%B6nnen

[1] https://www.dw.com/en/german-prosecutors-investigate-spyware-maker-finfisher/a-50293812#:~:text=The%20NGOs%20said%20there%20was,phones%2C%20according%20to%20the%20NGOs

تاریخ رمزنگاری لقب دادند. [1]

- **استانداردهای رمزنگاری تضعیف‌شده:** از منظر تاریخی، پس از جنگ سرد، ماجرای Crypto AG مقطعی یکتا بود. اما نگرانی درباره تعمد در تضعیف رمزنگاری توسط نهادهای اطلاعاتی همچنان وجود دارد. برای نمونه، در اوایل دهه ۲۰۱۰ بحث‌هایی پیرامون استانداردهای رمزنگاری NIST و احتمال وجود اعداد اول خاص تعبیه‌شده توسط NSA مطرح شد. آلمان در واکنش، رسماً اعلام کرد اجازه‌ی کارگزاری درِ پشتی در الگوریتم‌های رمز را نخواهد داد و حتی موضعی مخالف با خواست برخی کشورها (برای تضعیف رمزنگاری تجاری جهت دسترسی پلیس) اتخاذ کرد. در واقع، تجربه Rubikon موجب شده کارشناسان امنیتی آلمان نسبت به هر گونه ابهام در الگوریتم‌های رمزنگاری یا تراشه‌های رمزنگاری (نظیر ماجرای Infineonیادشده) با بدبینی و دقت بیشتری برخورد کنند. [2]
- **استفاده پلیس فدرال از جاسوس‌افزار Pegasus :** یکی از تازه‌ترین موارد، ورود مخفیانه‌ی جاسوس‌افزار بدنام «پگاسوس» به پلیس جنایی فدرال (BKA) است. به گزارش رسانه‌ها، BKA در سال ۲۰۱۹ به‌طور محرمانه نسخه‌ای تعدیل‌شده از Pegasus را از شرکت اسرائیلی NSO خریداری کرده و از سال ۲۰۲۱/۲۰۲۰ در موارد خاص به کار گرفته است. انگیزه‌ی این اقدام ناکامی چندساله‌ی پلیس در توسعه یا نصب مخفیانه‌ی تروجان بومی خود بود؛ مقامات در جلسه کمیسیون داخلی بوندستاگ اعتراف کردند که علی‌رغم عملکرد فنی تروجان داخلی، آن‌ها نتوانسته‌اند آن را بی‌سروصدا روی گوشی‌های هوشمند هدف نصب کنند و به‌دلیل تنوع و پیچیدگی سیستم‌های موبایل دچار مشکل شده‌اند. از این رو، BKAعلی‌رغم تردیدهای کارشناسان، به سراغ خرید Pegasus رفت. افشای موضوع در سپتامبر ۲۰۲۱ صورت گرفت؛ زمانی که در یک جلسه محرمانه پارلمانی، نمایندگان دولت تأیید کردند BKA این نرم‌افزار را تهیه کرده و »چندین بار «مورد استفاده قرار داده است. [3]

[1] https://www.zeit.de/politik/ausland/2020-02/bnd-cia-geheimdienste-verschluesselte-kommunikation-zdf#:~:text=beiden%20Geheimdienste%20sei%20es%20gelungen%2C,Mitarbeitenden%20verfasst%20wurden

[2] https://carnegieendowment.org/posts/2021/03/the-encryption-debate-in-germany-2021-update?lang=en#:~:text=The%20Encryption%20Debate%20in%20Germany%3A,on%20regulating%20encryption%20itself%2C

[3] https://www.zeit.de/politik/deutschland/2021-09/spionagesoftware-pegasus-bka-einsatz-nso-trojaner-israel#:~:text=Weil%20der%20eigene%20Staatstrojaner%20nicht,sind%20die%20rechtlichen%20Gefahren%20gro%C3%9F

۳ برخی شرکت‌های آلمانی فعال در صادرات تجهیزات نظارتی زیرساخت و خدمات حوزه فاوا

فهرست زیر برخی از شناخته‌شده‌ترین شرکت‌های آلمانی را شامل می‌شود که در حوزه زیرساخت مخابراتی، تجهیزات نظارتی و خدمات فناوری اطلاعات مدیریتی فعال بوده و محصولات یا خدمات خود را به خارج صادر کرده‌اند:

- **شرکت ترووِیکور Trovicor:** این شرکت مستقر در مونیخ ارائه‌دهنده‌ی مراکز مانیتورینگ و راهکارهای شنود قانونی است. ترووِیکور در واقع ادامه‌دهندهٔ بخش اطلاعات و شنود شرکت نوکیا زیمنس نت‌ورک (NSN)است. این شرکت سیستم‌های نظارت ارتباطات را به دولت‌ها و نیروهای امنیتی کشورهای مختلف می‌فروشد و در ادغام تجهیزات شنود در زیرساخت شبکهٔ اپراتورها تخصص دارد.
- **گاما گروپ/فین‌فیشِر Gamma Group/FinFisher:** یک شرکت آلمانی–بریتانیایی (دفتر مونیخ و لندن) که نرم‌افزارهای جاسوسی و بدافزارهای نظارتی تولید می‌کند. مهم‌ترین محصول آن‌ها اسب تروا FinSpy فین‌اسپای است که برای نفوذ به رایانه‌ها و موبایل‌ها و جمع‌آوری مخفیانه اطلاعات به کار می‌رود. این شرکت نرم‌افزارهای خود را هم به نهادهای امنیتی در اروپا (از جمله پلیس آلمان) و هم به دولت‌های خارجی فروخته است.
- **آتیس سیستمز ATIS systems:** این شرکت آلمانی مستقر در هومبورگ راهکارهای شنود قانونی و مدیریت اطلاعات ارتباطی ارائه می‌دهد. محصول اصلی آن‌ها با نام Klarios سیستم جامعی برای نظارت بر شبکه‌های تلفن و داده است. این شرکت سال‌ها در خاورمیانه و شمال آفریقا فعال بوده و ده‌ها سامانه نظارتی در کشورهای مختلف نصب کرده است.
- **اوتیماکو Utimaco:** این شرکت متخصص در زمینه سامانه‌های رهگیری قانونی (Lawful Interception) و ذخیره‌سازی داده‌های ارتباطی است. اوتیماکو نرم‌افزار مدیریتی LIMS را توسعه داده که قادر به رهگیری مکالمات تلفنی (همراه و ثابت) و ترافیک اینترنتی در مقیاس بسیار بزرگ است. محصولات این شرکت توسط دیگر تأمین‌کنندگان برای پیاده‌سازی مراکز نظارتی در کشورهای مختلف به‌کار گرفته شده است (مانند استفاده در پروژه‌های نظارت در ایران و سوریه)
- **الامان Elaman:** شرکتی آلمانی که به عنوان واسطه و شریک توزیع برخی فناوری‌های نظارتی (به‌ویژه محصولات گروه گاما فعالیت داشته است. مثلاً اسناد افشاشده نشان می‌دهد الامان در ارائه ابزارهای FinFisherبه بعضی کشورها (نظیر ترکمنستان) نقش داشته است.

۴ قوانین پشتیبان مرتبط با نظارت و شنود در کشور آلمان

در قوانین و مقررات کشور آلمان قوانینی وجود دارد که موضوع محدود سازی و شنود را برای نهادهای مشخصی تبدیل به امری قانونی می کند. از جمله این قوانین می توان به موارد زیر اشاره کرد.

I. قانون محدودسازی «اسرار نامه، پست و ارتباطات تلکام[۱]
(Gesetz zur Beschränkung des Brief-Post- und Fernmeldegeheimnisses – G-10-Gesetz)

- **موضوع:** محدود ساختن اصل «اسرار ارتباطی» (ماده ۱۰ قانون اساسی) در موارد استثنایی
- **محتوا:** دستگاه‌های اطلاعاتی فدرال (BND) و پلیس فدرال (BKA) می‌توانند **به‌رغمِ حقوق اساسی مردم** دسترسی به ترافیک تلفن، ایمیل و اینترنت را در شرایطی که مصلحت «امنیت خارجی» یا «ضدتروریسم» ایجاب کند، انجام دهند. استفاده از این قانون مشروط به صدور «مصوبه ویژه» از سوی وزارت کشور و نظارت دائمی یک مجلس ویژه می باشد.

II. قانون آیین دادرسی کیفری(Strafprozessordnung – StPO)

- § 100a StPO (Quellen-TKÜ)[۲]
  - شنود منبع: مجوز شنود صوت (تلفن) یا فیلتر DPI در مراکز مخابراتی با مجوز قاضی دادگاه صالح و «حداقل دلایل معتبر» در زمینه جرایم سنگین
- § 100b StPO (Online-Durchsuchung)[۳]
  - جست‌وجوی آنلاین: نصب و اجرای بدافزار حکومتی (Bundestrojaner) روی رایانه یا موبایل مظنون، بدون اطلاع او با حکم صریح قضائی، رعایت «تناسب میان هدف و تهاجم» و نظارت پسینی قوه قضائیه

III. قانون فدرال پلیس جنایی[۴](Bundeskriminalamt-Gesetz – BKAG)

- **موضوع:** اختیارات ویژه پلیس فدرال آلمان BKA برای اقدام در سطح ملی
- **ماده ۴:** امکان اجرای قانون جست‌وجوی آنلاین و اینترنتی توسط کارشناسان پلیس فدرال آلمان
- **ماده ۲۱:** همکاری اجباری اپراتورهای مخابراتی و فناوری اطلاعات با پلیس فدرال آلمان در زمینه شنود و استخراج داده

IV. قانون خدمات مخابراتی[۵](Telekommunikationsgesetz – TKG)

- موضوع: تعهد اپراتورها به پشتیبانی از «شنود قانونی (Lawful Interception) و ارائه امکانات فنی به نهادهای مجاز: اپراتورها باید زیرساخت‌های لازم را برای شنود مطابق حکم قضائی فراهم کنند، بی‌آنکه مشترک مطلع شود.

---

[1] https://www.bundestag.de/gremien/a06_commissions/g10
[2] https://www.gesetze-im-internet.de/stpo/__100a.html
[3] https://www.gesetze-im-internet.de/stpo/__100b.html
[4] https://www.gesetze-im-internet.de/bkag/__4.html , https://www.gesetze-im-internet.de/bkag/__21.html
[5] https://www.gesetze-im-internet.de/tkg_2004/__102.html,

V. قانون سرویس اطلاعات خارجی[1] (BND-Gesetz – BNDG)

- **موضوع**: اختیارات سرویس اطلاعات خارجی آلمان (BND) برای جمع‌آوری اطلاعات خارج از مرزهای آلمان
- **محتوا**: اجازه‌ی شنود، رصد و استخراج داده‌های دیجیتال اشخاص ثالث در خارج از کشور، بدون اطلاع آن‌ها با نظارت مجلس فدرال و دیوان دادگستری فدرال

[1] https://www.gesetze-im-internet.de/bndg/__15.html, https://www.bundestag.de/gremien/a03_lka/bndg

۵ جمع‌بندی (پیشنهادها):

با توجه به مطالب مطرح شده موارد زیر جهت اقدامات آتی پیشنهاد می شود:

۱) ارزیابی امنیتی و عملکردی مستمرّ کلیه تجهیزات و محصولات (نرم‌افزاری و برنامه‌های کاربردی) در حال استفاده در شبکه‌های مخابراتی و صنعتی کشور
۲) اعمال استانداردهای سخت‌گیرانه‌تر برای ارزیابی عملکردی و امنیتی محصولات وارداتی و خدمات خارجی با حساسیت بالا
۳) معرفی راه‌کارهای رفع خطرات امنیتی افشاشده در خصوص تجهیزات و محصولات در حال بهره‌برداری به کلیه بهره‌برداران مخابراتی، صنعتی و عمومی
۴) اطلاع‌رسانی مستمرّ در خصوص موارد مشابه به دستگاه‌های اجرایی فعال کشور در بخش‌های امنیتی، اطلاعاتی و تعاملات بین‌المللی

نشانی: تهران، انتهای کارگر شمالی، پژوهشگاه ارتباطات و فناوری اطلاعات، معاونت پژوهش و توسعه ارتباطات علمی

تلفن: ۰۲۱-۸۸۶۳۰۳۵۵

نمابر: ۰۲۱-۸۸۶۳۰۳۵۶