Quarterly Journal of Futures Studies, Modern Interdisciplinary Studies

AJA Imam Ali Military University https://www.ayandehpajoohi.ir/ Online ISSN: - Print ISSN: -

Analysis of Cyberattacks on Banks: A Focus on Recent Incidents and Security Measures in Iran

Rouhollah Moradi[1]✉ | Mina Arasteh[2] |Tanin Karimi Daghestani[3]|

1 .Assistant Professor, Department of Accounting, Faculty of Command and Management, Imam Ali (AS) Military University, Tehran, Iran. Email: financialmanagement4@gmail.com

2 .Corresponding Author, MA Student of Public Administration, Tehran, Iran. Email: minaaraste79@gmail.com

3. MA Student of Public Administration, Tehran, Iran. Email: karimitanin77@gmail.com

Article Info

Article type:

Research Article

Article history:

Received 25 March 2026

Received in revised form 16 June 2026

Accepted 16 June 2026

Published online 30 June 2026

Keywords:

Values, defense policymaking, defense-security policies

ABSTRACT

In recent years, the intensity and complexity of cyberattacks targeting critical infrastructure have increased dramatically, with the banking sector standing out as a primary and vulnerable target. Such attacks not only disrupt banking operations but also severely undermine public trusta cornerstone of economic stability and financial governance. This article analyzes recent cyberattacks on Iranian banks, focusing specifically on the large-scale attack against Bank Sepah, an incident that exposed critical weaknesses in the banking system's cyber preparedness and response capabilities. The study examines the technical, organizational, and psychological dimensions of these attacks, covering methods such as Distributed Denial-of-Service (DDoS) attacks, malware, social engineering, and unauthorized access to information systems. Furthermore, the attackers' objectives, the economic and security consequences, and the psychological impact of the attacks on society have been analyzed. Finally, by presenting a multi-layered framework, strategies are proposed to enhance cyber resilience and risk management within Iran's banking system. The findings indicate that addressing emerging threats requires coordinated collaboration among banks, government agencies, and information security specialists to safeguard stability and trust in the country's financial system. (Sadeghi, 2023; Gopalakrishnan & Trivedi, 2021)

Cite this article: Moradi, Rouhollah; Arasteh, Mina; Karimi Daghestani, Tanin (2026). Analysis of Cyberattacks on Banks with an Emphasis on Recent Attacks and Security Strategies in Iran. *Quarterly Journal of Futures Studies: Modern Interdisciplinary Studies*, 1(4), 4–18.

Publisher: AJA Imam Ali Military University

DOI: http//doi.org/000000000000000000

فصلنامه آینده‌پژوهی، مطالعات میان رشته‌ای نوین

دانشگاه افسری امام علی (ع)

https://www.ayandehpajoohi.ir/

Online ISSN: - Print ISSN: -

تحلیل حمله سایبری به بانک‌ها با تاکید بر حملات اخیر و راهکارهای امنیتی در ایران

روحا.. مرادی[1] مینا آراسته[2] ✉ طنین کریمی داغستانی[3]

۱. استادیار گروه حسابداری، دانشکده فرماندهی و مدیریت، دانشگاه افسری امام علی(ع)، تهران، ایران. رایانامه: financialmanagement4@gmail.com

۲.نویسنده‌مسئول،دانشجوی‌کارشناسی‌ارشدمدیریت‌ولتی،تهران،ایران،رایانامه:minaaraste79@gmail.com

۳. دانشجوی‌کارشناسی‌ارشدمدیریت‌ولتی،تهران،ایران،رایانامه:karimitanin77@gmail.com

اطلاعات مقاله

نوع مقاله:
مقالهٔ پژوهشی

تاریخ دریافت: ۱۴۰۴/۰۸/۰۱

تاریخ بازنگری: ۱۴۰۴/۱۱/۲۵

تاریخ پذیرش: ۱۴۰۴/۰۹/۳۰

تاریخ انتشار: ۱۴۰۵/۰۵/۳۱

کلیدواژه‌ها:
ارزش‌ها،سیاستگذاری دفاعی،سیاست‌های دفاعی-امنیتی

چکیده

در سال‌های اخیر، شدت و پیچیدگی حملات سایبری به زیرساخت‌های حیاتی به‌طور چشمگیری افزایش یافته است و نظام بانکی یکی از اهداف اصلی و آسیب‌پذیر این تهدیدات محسوب می‌شود. این حملات نه‌تنها تداوم عملیاتی بانک‌ها را با اختلال مواجه می‌کنند، بلکه اعتماد عمومی را نیز که از ارکان اساسی ثبات اقتصادی و حکمرانی مالی است، به‌شدت تضعیف می‌نمایند. مقاله حاضر به تحلیل حملات سایبری اخیر به بانک‌های ایران می‌پردازد و تمرکز ویژه‌ای بر حمله گسترده به بانک سپه دارد؛ حمله‌ای که نقاط ضعف جدی در آمادگی و واکنش سایبری نظام بانکی را آشکار ساخت. در این مطالعه، ابعاد فنی، سازمانی و روانی حملات بررسی می‌شود؛ از جمله روش‌هایی نظیر حملات توزیع‌شده انکار سرویس (DDoS)، بدافزارها، مهندسی اجتماعی و نفوذ به سامانه‌های اطلاعاتی. همچنین اهداف مهاجمان، پیامدهای اقتصادی و امنیتی، و تأثیر روانی حملات بر جامعه مورد تحلیل قرار گرفته است. در نهایت، با ارائه یک چارچوب چندلایه، راهکارهایی برای تقویت تاب‌آوری سایبری و مدیریت ریسک در نظام بانکی ایران پیشنهاد می‌شود. یافته‌ها نشان می‌دهند که مقابله با تهدیدات نوظهور نیازمند همکاری هماهنگ بین بانک‌ها، نهادهای دولتی و متخصصان امنیت اطلاعات است تا از ثبات و اعتماد در نظام مالی کشور محافظت شود. (صادقی، ۱۴۰۲؛ Gopalakrishnan & Trivedi 2021,)

استناد: مرادی، روحا..؛ آراسته، مینا؛ کریمی داغستانی، طنین (۱۴۰۴). تحلیل حمله سایبری به بانک‌ها با تاکید بر حملات اخیر و راهکارهای امنیتی در ایران. فصلنامه *آینده پژوهی مطالعات میان رشته‌ای نوین*، ۱ (۴)، ۴-۱۸.

ناشر: دانشگاه افسری امام علی (ع)

DOI: DOI: http//doi.org/0000000000000000000000000

مقدمه

امروزه زیرساخت‌های دیجیتال به ستون فقرات نظام‌های اقتصادی و سیاسی تبدیل شده‌اند. در این میان، نظام بانکی یکی از اصلی‌ترین اهداف مهاجمان سایبری در سراسر جهان است. بانک‌ها نه‌تنها به عنوان مراکز نگهداری سرمایه‌های مردم بلکه به عنوان نقطه اتصال میلیون‌ها کاربر به اقتصاد کلان و خرد، اهمیت حیاتی دارند.

ایران نیز در سال‌های اخیر با توسعه بانکداری الکترونیکی، گسترش خدمات آنلاین، پرداخت‌های دیجیتال و سامانه‌های یکپارچه بین‌بانکی، وابستگی شدیدی به زیرساخت‌های فناوری پیدا کرده است.

این در حالی است که موقعیت ژئوپلیتیکی ایران، شرایط تحریمی، جنگ‌های نیابتی و رقابت‌های منطقه‌ای، این کشور را به یکی از اهداف دائمی جنگ‌های ترکیبی و حملات سایبری سازمان‌یافته تبدیل کرده است. (مؤسسه افتا، ۱۴۰۱)

در جنگ‌های ترکیبی مدرن، که ابعاد نظامی، اقتصادی، و اطلاعاتی در هم تنیده‌اند، سیستم‌های بانکی به عنوان شریان حیاتی اقتصاد و پشتیبان عملیات نظامی، به اهداف استراتژیک حملات سایبری تبدیل می‌شوند (Deibert, 2022) .

تجربه اخیر جنگ ۱۲ روزه ایران و رژیم صهیونیستی و حمله سایبری گروه "گنجشک درنده" به بانک سپه، مصداق بارزی از این واقعیت تلخ است. این حمله نه تنها به اختلال گسترده در عملیات بانکی و پرداخت حقوق پرسنل نظامی منجر شد، بلکه پس از گذشت یک ماه، بانک هنوز نتوانسته به حالت عادی بازگردد، که نشان‌دهنده عمق آسیب‌پذیری و پیامدهای فلج‌کننده چنین حملاتی است. این رخداد از چند منظر اهمیت دارد:

_میزان آمادگی زیرساختی و فنی شبکه بانکی را به چالش کشید.

_نقطه‌ضعف‌های امنیتی را نمایان کرد.

_ابعاد روانی و اجتماعی حملات سایبری را آشکارتر کرد.

و نشـــان داد کـــه جنگ‌هـــای مـــدرن، فراتـــر از میـــدان‌های نظـــامی ســـنتی بـــه زیرساخت‌های اقتصادی کشیده شده‌اند.

هـدف از ایـن ارائـه، بررسـی تحلیلـی آسـیب‌پذیری‌های کلیـدی سیسـتم‌های بـانکی در مواجهـه بـا جنگ‌هـای سـایبری و ارائـه راهکارهـای عملـی و اسـتراتژیک بـرای تقویت تـاب‌آوری سـایبری و تـداوم کسـب‌وکار در مواجهـه بـا ایـن تهدیـدات نوظهـور است. رویکرد مـا در ایـن نوشـتار فراتـر از ملاحظـات صـرفاً فنـی بـوده و شـامل ابعـاد مالی، حسابداری، و حکمرانی سایبری نیز می‌شود.

بیان مسئله و پیشینه‌های پژوهش

بیان مسئله

رخدادهایی مانند حمله سایبری گسترده به بانک سپه در جریان جنگ سایبری اخیر میان ایران و رژیم صهیونیستی، بار دیگر ضعف زیرساختی و مدیریتی سیستم بانکی ایران در برابر تهدیدات سـایبری را نمایان سـاخت. این حمله نه تنها موجب توقف پرداخت حقوق نیروهای نظامی شـد، بلکه حتی پس از یک ماه، بانک به وضعیت عادی بازنگشت؛ موضوعی که آسیب‌پذیری شدید را نشان می‌دهد(خبرگزاری مهر، ۱۴۰۴؛۲۰۲۲,Reuters)

پیشینه پژوهش

مطالعات داخلی و خارجی متعددی به بررســـی تهدیدات ســـایبری علیه زیرســـاخت‌های مالی پرداخته‌اند. شـــریفی و همکاران (۱۳۹۹) به چالش‌های امنیت ســـایبری در بلنک‌های ایرانی پرداخته و ضعف در آموزش منابع انسانی و نبود سامانه‌های تشخیص تهدید را مهم‌ترین عوامل آسـیب‌پذیری دانسـته‌اند. در سـطح بین‌المللی، گزارش (Akamai 2021)و پژوهش(IBM 2023)نشان می‌دهد که صنعت مالی دومین هدف مهم حملات DDOS و باج‌افزاری در سال‌های اخیر بوده است.

چارچوب نظری

چارچوب نظری این پژوهش بر مفاهیم «تاب‌آوری سـایبری (Cyber Resilience)» و «مدیریت ریسک سایبری» استوار است. طبق نظریه‌های امنیت اطلاعات(Whitman & Mattord, 2022) ، سـیسـتم‌های بانکی باید بتوانند در برابر حملات سـایبری مقاومت کرده و در صـورت اختلال، بازیابی ســـریع اطلاعات و خدمات را تضـــمین نمایند. همچنین نظریه «حاکمیت ســـایبری «

(Cyber Governance) نیز بر اهمیت سیاست‌گذاری شفاف و همکاری نهادی در مقابله با تهدیدات تأکید دارد.(Von Solms & Van Niekerk, 2013)

شرح حملات سایبری

بر اساس گزارش‌ها، در این حملات، چندین بانک بزرگ و متوسط کشور درگیر شدند؛ از جمله بانک‌های سپه، پاسارگاد و ملت. طی چند روز، بسیاری از کاربران اعلام کردند که دسترسی به سامانه‌های اینترنت بانک یا همراه بانک قطع شده یا به کندی انجام می‌شود. بعضی از تراکنش‌های آنلاین با اختلال شدید مواجه شد (ایسنا، ۱۴۰۴). در مواردی حتی شایعاتی درباره نفوذ به اطلاعات مشتریان در فضای مجازی دست‌به‌دست شد .

روش‌های حمله

اطلاعات رسمی منتشر شده محدود است؛ اما شواهد و تحلیل‌های فنی برخی کارشناسان مستقل نشان می‌دهد که مدل اصلی این حملات از نوع حمله توزیع‌شده منع سرویس (DDOS)بوده است. در این روش، مهاجمان با استفاده از هزاران یا میلیون‌ها سیستم آلوده (بات‌نت) به سرورهای هدف، درخواست‌های متعدد و جعلی ارسال می‌کنند. سرورها به دلیل ترافیک مصنوعی بسیار بالا، دیگر نمی‌توانند پاسخ‌گوی کاربران واقعی باشند . (Cloudflare, 2023)

این نوع حملات نیاز به تجهیزات پیشرفته ندارد اما در صورت ضعف زیرساخت شبکه یا پهنای باند ناکافی، بسیار مؤثر واقع می‌شود. مهاجمان اغلب سرورهای پراکسی، VPN، ربات‌های شبکه‌های اجتماعی یا حتی دستگاه‌های IoT ناایمن را برای ایجاد شبکه بات‌نت مورد استفاده قرار می‌دهند.

برخی گمانه‌زنی‌ها حاکی از تلاش برای نفوذ مستقیم به پایگاه‌های داده نیز بود، ولی طبق اطلاعیه‌های رسمی، بانک‌ها ادعا کردند که نفوذ مستقیم به داده‌ها صورت نگرفته است. با این حال، در فضای سایبری، گاهی حتی شایعه افشای اطلاعات، به اندازه حمله واقعی، اثر روانی دارد (Computer Emergency Response Team –Iran CERT, 2023) .

اهداف و ابعاد حمله

اهداف آشکارحملات سایبری به بانک‌ها اهداف متعددی را دنبال می‌کنند:

۱ .ایجاد نارضـــایتی اجتماعی: وقتی مردم نتوانند پول جابجا کنند یا موجودی حســـاب خود را ببینند، دچار استرس، بی‌اعتمادی و نگرانی می‌شوند (Schneier, 2020) .
۲ .ضـربه به اعتماد عمومی: اعتماد به نظام بانکی بخش مهمی از سـرمایه اجتماعی یک کشـور است؛ تخریب آن می‌تواند آثار اقتصادی بلندمدت داشته باشد(صادقی، ۱۴۰۲).
۳ .برهم زدن امنیت اقتصـــادی: در صـــورت موفقیت‌آمیز بودن حملات، امکان ایجاد بحران نقدینگی و حتی افزایش گردش پول نقد در سطح جامعه وجود دارد (IMF, 2022) .
۴ .ایجاد جنگ روانی: بســـیاری از گروه‌های هکری با حمایت دولت‌ها یا به‌صـــورت پیمان‌کاران سایبری عمل می‌کنند و حمله به زیرساخت‌های مالی، بخشی از جنگ ترکیبی آنهاست (Rid, 2020) .

ابعاد آسیب‌ها

حتی در صورت مهار سریع حملات، پیامدهای زیر را نمی‌توان نادیده گرفت:
ـ کند شدن دسترسی‌ها در دوره اوج حملات
ـ هزینه‌های سنگین فنی برای تقویت موقت زیرساخت‌ها
ـ هزینه‌های روابط عمومی و جلب دوباره اعتماد مشتریان
ـ آسیب به برند و اعتبار برخی بانک‌ها.(PwC, 2021)

دلایل آسیب‌پذیری سیستم بانکی ایران

در ارزیابی چرایی موفقیت نسبی این حملات، سه عامل اصلی را می‌توان برشمرد:

۱. وابستگی بیش‌ازحد به زیرساخت‌های متمرکز فناوری اطلاعات

شـــرح آســـیب‌پذیری: بانک‌های مدرن به شـــدت به شـــبکه‌های متمرکز، پایگاه‌های داده عظیم، سـیسـتم‌های پرداخت برخط، و سـامانه‌های بین‌بانکی وابسـته هسـتند. این تمرکز، نقطه‌ای واحد برای شکست ایجاد می‌کند.
پیامدها: اختلال در این زیرساخت‌ها، می‌تواند زنجیره مالی نیروهای مسلح را فلج کرده، عملیات نظامی را مختل سازد و اعتماد عمومی به سیسـتم بانکی و حتی دولت را به شـدت کاهش دهد. حمله به بانک سپه که پرداخت حقوق پرسنل نظامی را متوقف کرد، نمونه بارز این پیامد است.
ریسـک مالی و حسـابداری: اختلال در ثبت و پردازش تراکنش‌ها منجر به عدم تطابق حسـاب‌ها، افزایش هزینه‌های عملیاتی برای بازیابی، و زیان‌های ناشی از عدم ارائه خدمات می‌شود. (Kaspersky, 2023)

۲. عدم جداسازی مؤثر سیستم‌های حیاتی و حساس:

شرح آسیب‌پذیری: برخی سامانه‌های حیاتی، مانند سیستم‌های پرداخت حقوق نظامیان یا پایگاه‌های داده محرمانه مالی، به دلیل ملاحظات دسترسی یا مدیریت اشتباه، به اینترنت عمومی یا شبکه‌های پرریسک متصل باقی می‌مانند .

پیامدها: این اتصال ناامن، درهای نفوذ را برای گروه‌های هکری پیچیده مانند "گنجشک درنده" باز می‌کند. اطلاعات فاش شده حاکی از آن است که نفوذ به بانک سپه احتمالاً از طریق نقاط ضعف در اتصالات اینترنتی یا واسطهای ارتباطی نامطمئن رخ داده است.

ریسک عملیاتی و امنیتی: نفوذ به این سیستم‌ها علاوه بر افشای اطلاعات محرمانه، می‌تواند به تغییر داده‌های مالی، دستکاری در پرداخت‌ها، و ایجاد عدم قطعیت در وضعیت مالی نهادهای حساس منجر شود(Kaspersky, 2023).

۳. تأخیر و ضعف در مدیریت وصله‌های امنیتی و به‌روزرسانی‌ها:

شرح آسیب‌پذیری: بسیاری از بانک‌ها به دلیل نگرانی از اختلال در عملیات جاری یا پیچیدگی فرآیند، به‌روزرسانی‌های امنیتی و نصب وصله‌های حیاتی را به تعویق می‌اندازند

پیامدها: وجود آسیب‌پذیری‌های شناخته‌شده در نرم‌افزارها و سخت‌افزارهای قدیمی، فرصتی طلایی برای بهره‌برداری مهاجمان فراهم می‌کند. باگ‌های نرم‌افزاری قدیمی در سیستم‌های بانک سپه از جمله نقاط ورود اولیه برای حمله سایبری بوده‌اند.

ریسک تطبیق‌پذیری: عدم رعایت استانداردهای به‌روز امنیتی و مدیریت وصله‌ها، ریسک‌های حقوقی و نظارتی را نیز افزایش می‌دهد.(Symantec, 2022) .

۴. فقدان استراتژی جامع پشتیبان‌گیری، بازیابی و تداوم کسب‌وکار:

شرح آسیب‌پذیری: نداشتن نسخه‌های پشتیبان امن، رمزنگاری شده و خارج از سایت و همچنین فقدان طرح‌های بازیابی در شرایط بحرانی (Disaster Recovery Plan) که به طور منظم تست شوند .

پیامدها: حملاتی مانند باج‌افزار می‌توانند داده‌ها را به طور کامل نابود یا غیرقابل دسترسی کنند. بانک سپه به دلیل عدم وجود نسخه‌های پشتیبان معتبر و طرح بازیابی مؤثر، در بازگشت سریع به حالت عادی ناکام ماند و به دلیل از دست رفتن داده‌ها، عملیات مالی مختل شد.

ریسک مالی: خسارات ناشی از از دست رفتن داده‌ها، هزینه‌های بازسازی سیستم‌ها و پرداخت جریمه‌های تأخیر در خدمات می‌تواند بسیار گزاف باشد(ENISA,2020) .

۵. ضعف در سیستم‌های هشدار سریع، پایش و تحلیل رفتار:

شـــرح آســـیب‌پذیری: عدم اســـتقرار ســـامانه‌های مدیریت اطلاعات و رویدادهای امنیتی و سیستم‌های تحلیل رفتار کاربران و نهادها یا استفاده ناکافی از آن‌ها.

پیامدها: فقدان دید کافی بر فعالیت‌های مشکوک در شبکه و سیستم‌ها، باعث می‌شود حملات تا زمان وارد آمدن خسارت سنگین یا حتی فلج شدن کامل سیستم شناسایی نشوند. در مورد بانک سپه، حمله تا زمان ایجاد اختلال گسترده شناسایی نشد، که نشان‌دهنده نبود مکانیزم‌های تشخیص زودهنگام بود.

ریسک حسابرسی: ناتوانی در ثبت و تحلیل رویدادهای امنیتی، روند حسابرسی داخلی و خارجی را مختل کرده و امکان ردیابی دقیق منشأ حملات را دشوار می‌ساز(IBM,۲۰۲۳).

۶. آگاهی پایین کارکنان و ریسک خطای انسانی:

شرح آسیب‌پذیری: کارکنان بدون آموزش کافی در زمینه امنیت سایبری، ممکن است طعمه حملات فیشینگ، مهندسی اجتماعی، یا استفاده از رمزهای عبور ضعیف و شیوه‌های ناامن ارتباطی شوند .

پیامدها: حملات فیشینگ یا مهندسی اجتماعی به راحتی موفق می‌شوند و اغلب نفوذ اولیه به سیستم‌ها از این طریق صورت می‌گیرد. احتمالاً نفوذ اولیه به بانک سپه نیز از طریق همین نقاط ضعف انسانی رخ داده است.

ریسک تطبیق‌پذیری: عدم رعایت پروتکل‌های امنیتی توسط کارکنان، مسئولیت‌پذیری سازمان را در برابر نقض داده‌ها افزایش می‌دهد(موسوی، ۱۴۰۰)

۷. فقدان سامانه‌های پشتیبان عملیاتی (Hot Backup) و قابلیت دسترسی بالا:

شرح آسیب‌پذیری: عدم وجود دیتاسنترهای موازی با قابلیت سوئیچینگ خودکار و سیستم‌های فعال همزمان در جغرافیای مختلف

پیامدها: در صورت حمله یا از کار افتادن دیتاسنتر اصلی، قطع کامل خدمات بانکی رخ می‌دهد. ناتوانی بانک سپه در بازگشت سریع به دلیل نبود سیستم جایگزین و فعال همزمان، گواه این آسیب‌پذیری است.

ریسک تداوم کسب‌وکار: این فقدان مستقیماً بر تداوم خدمات مالی حیاتی و توانایی بانک در ایفای تعهدات خود به مشتریان و نهادهای نظامی تأثیر می‌گذارد(Microsoft Security,2021) .

به طور کلی دلایل آسیب پذیری سیستم بانکی ایران بدین شرح است :

۱ .زیرساخت‌های قدیمی

بسیاری از بانک‌های ایرانی از نرم‌افزارها و سخت‌افزارهایی استفاده می‌کنند که در دهه‌های گذشته طراحی شده‌اند و طی سال‌ها تغییرات متعدد روی آنها اعمال شده است. این سیستم‌ها اغلب با تکنولوژی‌های جدید به‌طور کامل سازگار نیستند و در برابر برخی حملات، آسیب‌پذیرترند.

۲ .کمبود نیروی متخصص امنیت سایبری

یکی از پیامدهای تحریم‌ها و چالش‌های داخلی، مهاجرت نیروهای کارآزموده است. بانک‌ها برای مقابله با حملات گسترده نیازمند تیم‌های قوی امنیتی ۲۴ ساعته هستند که طراحی، پیش‌بینی و مانیتورینگ دائمی انجام دهند. کمبود این نیروها، سطح دفاعی بانک‌ها را کاهش می‌دهد.

۳ .ضعف هماهنگی بین‌سازمانی

در بسیاری از کشورها، بانک مرکزی، مرکز CERT ملی و نهادهای قضایی و امنیتی، یک شبکه واکنش سریع یکپارچه دارند. در ایران اگرچه نهادهایی مانند مرکز مدیریت راهبردی افتا، پلیس فتا و شرکت‌های امنیتی خصوصی فعال‌اند، اما بعضا نبود هماهنگی و دستورالعمل‌های لحظه‌ای باعث تأخیر در واکنش می‌شود.

تجربه‌ها و اقدامات مقابله‌ای

در برابر چنین حملاتی، واکنش سریع و مدیریت بحران اهمیت زیادی دارد. بانک‌ها برای مقابله با موج حملات سایبری اخیر اقدامات زیر را اجرا کردند:

_افزایش پهنای باند دیتاسنترها برای مقاومت در برابرDDOS

_استفاده از سامانه‌های Anti-DDOS داخلی و همکاری با اپراتورهای اینترنت

_محدود کردن دسترسیIP های خارجی یا مشکوک

_اطلاع‌رسانی عمومی به مشتریان و راه‌اندازی خطوط پشتیبان

_افزایش بازرسی‌های امنیتی داخلی(مرکز افتا، ۱۴۰۲؛ پلیس فتا، ۱۴۰۲).

مرکز مدیریت راهبردی افتا و پلیس فتا نیز اعلام کردند حملات در حال پایش دائمی است و برخی سرنخ‌های مهاجمان شناسایی شده‌اند.

تجربه‌های مشابه قبلی مانند حمله سایبری به جایگاه‌های سوخت در سال ۱۴۰۰ یا حملات به برخی وزارتخانه‌ها نشـــان داده‌اند که نقاط ضـــعف فنی قابل تکرار اســـت و اگر در دوره آرامش تقویت نشود، در بحران‌ها دوباره آشکار می‌شود. (خبرگزاری مهر ,۱۴۰۴).

تجربه سایر کشورها و مقایسه تطبیقی

تجربه کشورهای مختلف نشان می‌دهد که حملات سایبری به بانک‌ها تنها مختص ایران نیست، بلکه بخشی از واقعیت جنگ‌های نوین است.

در ســال ۲۰۲۲، هم‌زمان با جنگ اوکراین، چندین بانک اروپای شــرقی از جمله در لهســتان و اسلواکی هدف حملات DDoS قرار گرفتند. با این حال، این کشورها با بهره‌گیری از شبکه‌های جهانی مقابله با حمله مانند Akamai و Cloudflare موفق شـــدند از تداوم اختلال جلوگیری کنند.(Cloudflare, 2022)

در کره‌جنوبی، در سال ۲۰۱۳ یک حمله سایبری گسترده به بانک‌ها و رسانه‌ها صورت گرفت که موجب فلج شـــدن ســـامانه‌های اطلاعاتی شـــد. پس از این رویداد، دولت کره جنوبی اقدام به بازنویســـی قوانین امنیت ســـایبری کرد و ســـرمایه‌گذاری قابل توجهی در زیرســـاخت‌های دفاع سایبری انجام داد.(Park et al. 2014)

روسیه نیز از سال‌ها پیش، هدف حملات مداوم سایبری بوده است و در پاسخ، زیرساخت‌های مالی خود را با اســـتفاده از شـــبکه داخلی و ذخیره داده‌های محلی ایمن‌ســـازی کرده اســـت. همچنین همکاری بین‌بانکی با نهادهای امنیتی در روسیه بسیار پیشرفته است (2020Chertoff & Simon,).

این نمونه‌ها نشـــان می‌دهد که مقابله با حملات ســـایبری نیازمند برنامه‌ریزی ســـاختاریافته، تجهیزات به‌روز و همکاری نهادی مؤثر است.

راهکارها و پیشنهادها

برای مقابله مؤثر با این تهدیدات، یک رویکرد چندلایه و جامع، شـــامل ابعاد فنی، فرآیندی، و انسانی، ضروری است:

۱. ایزولاسیون کامل شبکه‌های حساس:

راهکار: جداســـازی کامل و فیزیکی ســـامانه‌های مالی و نظامی حیاتی از اینترنت عمومی و شـــبکه‌های داخلی با ریســـک بالا، با اســـتفاده از شـــبکه‌های داخلی مســـتقل و اختصـــاصـــی و

پیاده‌سازی سخت‌گیرانه تقسیم‌بندی شبکه برای جداسازی بخش‌های مختلف بانک و محدود کردن حرکت جانبی مهاجم در صورت نفوذ اولیه.
اقدام پیشنهادی: ایجاد زیرساخت‌های ابری خصوصی و مجزا برای سیستم‌های پرداخت حقوق و مزایای نیروهای نظامی، با پروتکل‌های امنیتی اختصاصی و عدم دسترسی مستقیم از اینترنت.
مزیت: کاهش چشمگیر نقاط ورودی برای حملات سایبری و محدود کردن دامنه خسارت در صورت نفوذ(ENISA,۲۰۲۰) .

۲. مدیریت وصله و به‌روزرسانی مداوم و خودکار:
راهکار: اعمال سیاست‌های سختگیرانه برای به‌روزرسانی منظم و اجباری سیستم‌عامل‌ها، پایگاه‌های داده، نرم‌افزارهای مالی و تمامی اجزای زیرساختی. استفاده از راهکارهای مدیریت آسیب‌پذیری برای شناسایی و رفع فعالانه نقاط ضعف.
اقدام پیشنهادی: پیاده‌سازی سیستم‌های خودکار مدیریت وصله و تست آن‌ها در محیط‌های ایزوله قبل از اعمال در سیستم اصلی. اولویت‌بندی به‌روزرسانی‌های مرتبط با آسیب‌پذیری‌های حیاتی و عمومی شناخته‌شده.
مزیت: کاهش آسیب‌پذیری‌های شناخته‌شده و بستن راه‌های نفوذ مهاجمان که اغلب از نقاط ضعف عمومی بهره‌برداری می‌کنند(Microsoft Security,.۲۰۲۱)

۳. طراحی و تست جامع استراتژی‌های تداوم کسب‌وکار و بازیابی فاجعه:
راهکار: تدوین طرح‌های جامع تداوم کسب‌وکار و بازیابی در شرایط بحرانی با تمرکز بر بازه زمانی هدف بازیابی و نقطه بازیابی هدف نزدیک به صفر.
اقدام پیشنهادی: ذخیره نسخه‌های پشتیبان رمزنگاری شده و تغییرناپذیر در چندین مرکز داده خارج از سایت و مناطق جغرافیایی متفاوت. انجام تست‌های دوره‌ای و شبیه‌سازی بحران برای اطمینان از کارایی طرح‌ها در عمل.
مزیت: تضمین بازیابی سریع و کامل داده‌ها و خدمات پس از حملات مخرب مانند باج‌افزار، و حفظ تداوم عملیات بانکی (ISO/IEC,2019)

۴. استقرار سامانه‌های تحلیل تهدید و هوش سایبری پیشرفته:
راهکار: پیاده‌سازی سیستم‌های پیشرفته SIEM و پلتفرم‌های هماهنگی، خودکارسازی و پاسخ‌دهی امنیتی **(**SOAR**)** برای نظارت لحظه‌ای، تحلیل رفتارهای مشکوک و پاسخ خودکار به تهدیدات.

اقدام پیشـــنهادی: ادغام پلتفرم‌های هوش تهدید (Threat Intelligence Platforms) برای جمع‌آوری و تحلیل اطلاعات به‌روز در مورد مهاجمان، تاکتیک‌ها، تکنیک‌ها و رویه‌های آن‌ها و اشتراک‌گذاری فعال اطلاعات با سایر بانک‌ها، نهادهای امنیتی و نظامی.
مزیت: تشـــخیص زودهنگام حملات، کاهش زمان پاســـخ و جلوگیری از گســـترش آســـیب. (IBM,2023)

۵. ارتقاء آگاهی و آموزش پیشرفته کارکنان و تمرین‌های شبیه‌سازی:
راهکار: برگزاری دوره‌های آموزشـــی مســـتمر و پیشـــرفته امنیت ســـایبری برای تمامی ســـطوح کارکنان، با تمرکز بر تهدیدات واقعی مانند فیشـــینگ، مهندســـی اجتماعی، و مدیریت قوی رمز عبور.
اقدام پیشنهادی: اجرای تمرین‌های دوره‌ای شبیه‌سازی حملات سایبری و تست نفوذ اجتماعی برای آمادگی کارکنان در شرایط واقعی و تبدیل آن‌ها به اولین خط دفاعی.
مزیت: کاهش چشـــمگیر خطاهای انســـانی به عنوان یکی از رایج‌ترین نقاط ضـــعف در حملات سایبری(SANS Institute,2022) .

۶. پیاده‌سازی فناوری‌های نوین امنیت:
راهکار: بررســـی و پیاده‌ســـازی ســـیســـتم‌های پرداخت و ثبت تراکنش‌های حســـاس مبتنی بر بلاک‌چین خصـــوصـــی با رمزنگاری چندلایه و الگوریتم‌های قوی برای افزایش شـــفافیت، تغییرناپذیری و امنیت.
اقدام پیشنهادی: طراحی و استفاده از پروتکل‌های امضای دیجیتال چندمرحله‌ای و تأیید هویت چندعاملی برای تمامی تراکنش‌های حساس، به ویژه در پرداخت‌های نظامی.
مزیت: افزایش امنیت، شـــفافیت و اثبات‌پذیری تراکنش‌های مالی، کاهش خطر دســـتکاری داده‌ها (Zyskind et al.,2015) .

۷. تقویت همکاری‌های بین‌سازمانی و سایبری:
راهکار: تشکیل کمیته‌های مشترک امنیت سایبری بانکی-نظامی با حضور متخصصان ارشد از هر دو بخش برای هماهنگی دفاعی و اشتراک اطلاعات تهدید.
اقدام پیشنهادی: برگزاری رزمایش‌های سایبری مشترک بین سیستم بانکی و نهادهای دفاعی، و توسعه پروتکل‌های پاسخ سریع و بازیابی هماهنگ در سطح ملی. ایجاد کانال‌های ارتباطی امن و سریع برای تبادل اطلاعات در زمان بحران.

مزیت: ایجاد یک دفاع سایبری یکپارچه و هماهنگ در برابر حملات ترکیبی و افزایش تاب‌آوری ملی(Cybersecurity & Infrastructure Security Agency, 2022) .

۸. ایجاد سامانه‌های پشتیبان عملیاتی همزمان و دیتاسنترهای توزیع‌شده:

راهکار: استقرار دیتاسنترهای موازی و فعال همزمان در چندین منطقه جغرافیایی مختلف با قابلیت سوئیچینگ خودکار و بدون وقفه در شرایط بحران.

اقدام پیشنهادی: سرمایه‌گذاری در زیرساخت‌های ابری توزیع‌شده که امکان تداوم خدمات را حتی در صورت از کار افتادن یک منطقه کامل فراهم می‌کند. طراحی معماری با قابلیت تحمل خطا در تمامی سطوح.

مزیت: کاهش زمان قطعی خدمات به حداقل ممکن در هنگام حملات شدید و تضمین تداوم عملیات حیاتی (Google Cloud Security,2021).

به طور کلی راهکارهای جامع مقابله با تهدیدات سایبری و تقویت تاب‌آوری بانکی بدین شرح است:

به‌روزرسانی زیرساخت‌ها:

تجهیز بانک‌ها به فایروال‌های هوشمند، سامانه‌های کشف نفوذ(IDS/IPS) ، سامانه‌های تحلیل ترافیک، بکاپ‌گیری امن و پهنای باند رزرو ضروری است.

آموزش نیروی انسانی:

سرمایه‌گذاری در تربیت و نگه‌داشت نیروهای متخصص و طراحی مشوق برای جلوگیری از مهاجرت آنان.

تدوین نقشه واکنش سریع:

ایجاد «اتاق جنگ سایبری» با پروتکل‌های دقیق بین بانک‌ها، بانک مرکزی، افتا و پلیس فتا.

آگاهی‌رسانی عمومی:

اطلاع‌رسانی شفاف و به‌موقع به مشتریان برای جلوگیری از انتشار شایعات، کاهش فشار روانی و جلوگیری از مهندسی اجتماعی.

همکاری بین‌المللی:

در شرایطی که تحریم‌ها اجازه دهد، می‌توان از تجربه و تجهیزات شرکت‌های معتبر امنیت سایبری دنیا بهره برد.

تحلیل مالی پیامدهای حملات سایبری بر نظام بانکی ایران

حملات سایبری به بانک‌ها فقط یک چالش فنی نیست، بلکه تبعات مستقیم و غیرمستقیم مالی دارد که می‌تواند ســـودآوری و عملکرد عملیاتی بانک‌ها را تحت تأثیر قرار دهد. این اثرات را می‌توان در سه دسته بررسی کرد:

۱ .هزینه‌های مستقیم دفاع و بازیابی

بانک‌ها مجبور می‌شـوند برای بازگرداندن ســرویس‌ها به وضـعیت پایدار، هزینه‌های غیرمنتظره بپردازند. این هزینه‌ها شامل:

_اجاره پهنای باند اضافی و تجهیزاتAnti-DDOS

_جذب مشاوران امنیتی و پیمان‌کاران فنی

_افزایش هزینه‌های نگهداری دیتاسنترها

_تست و ارزیابی مجدد زیرساخت‌های امنیتی پس از حمله

_هزینه‌های جبران خسارت در صورت بروز خطاهای داخلی یا زیان مشتریان.(PwC, 2021)

۲ .کاهش درآمدهای عملیاتی

در دوره حمله، بسـیاری از تراکنش‌های آنلاین کاهش پیدا می‌کند. این امر می‌تواند روی درآمد کارمزد خدمات بانکی اثر منفی داشته باشد. بانک‌های ایرانی به‌طور میانگین بخشی از سود خود را از محل کارمزد تراکنش‌های کارت‌خوان، اینترنت‌بانک و خدمات غیرحضـوری تأمین می‌کنند. هر اختلال مستقیم باعث کاهش این درآمد می‌شود.

۳ .آثار بلندمدت بر اعتبار و ارزش بازار

بانک‌ها شرکت‌های عمومی هستند و در بازار سرمایه سهام‌داران دارند. کاهش اعتماد مشـتریان می‌تواند ریزش تعداد مشـتریان، خروج سـپرده‌گذاران بزرگ و کاهش سـهم بازار را در پی داشـته باشد.

همچنین در صورت تشدید بحران و نیاز به تزریق منابع برای جبران خسارت‌ها، نسبت‌های مالی بانک مانند کفایت سـرمایه، بازده حقوق صـاحبان سـهام و نسـبت‌های نقدینگی تحت فشـار قرار می‌گیرند. (IMF,2022) .

تحلیل مدیریت مالی بحران و کنترل ریسک

یکی از اصـول مدیریت مالی مدرن، شـناسـایی و مدیریت انواع ریسـک‌های سـیسـتماتیک و غیرسیستماتیک است. در این چارچوب، حملات سایبری یک ریسک عملیاتی و همزمان ریسک اعتباری برای بانک‌ها محسوب می‌شود.

اقدامات ضروری مدیریت مالی در چنین بحران‌هایی:

۱ .تشکیل ذخیره ریسک سایبری:

بانک‌ها می‌توانند بخشـی از سـود انباشـته یا ذخایر اختیاری را برای پوشـش هزینه‌های احتمالی حملات سـایبری اختصـاص دهند. این ذخیره می‌تواند طبق اسـتانداردهای حسـابداری به‌عنوان هزینه‌های پیش‌بینی‌نشده لحاظ شود .(IFRSFoundation, 2021)

۲ .بیمه سایبری:

در بسـیاری از کشـورها بانک‌ها از بیمه‌های خاص برای جبران خسـارت‌های ناشـی از حملات سـایبری اسـتفاده می‌کنند. در ایران این ابزار هنوز فراگیر نیسـت و نیازمند توسـعه اسـت . (2023Allianz Cyber Report,).

۳ .مدیریت نقدینگی:

در شـرایط بحران سـایبری، احتمال افزایش برداشـت‌های غیرمنتظره نقدی وجود دارد. بانک‌ها باید برنامه‌های مدیریت نقدینگی کوتاه‌مدت داشـته باشـند تا بحران تبدیل به بحران نقدینگی نشود.(BCBS, 2022) .

۴ .شفافیت مالی:

انتشار گزارش‌های مالی شفاف پس از حمله سایبری می‌تواند از هجوم شایعات جلوگیری کند و آرامش را به بازار سرمایه بازگرداند. (FRC,2023)

۵ .بازنگری در بودجه‌های فناوری اطلاعات:

یکی از مهم‌ترین اقدامات مدیریت مالی، اختصـاص بودجه کافی برای پروژه‌های امنیت سـایبری اسـت. هزینه‌های امنیت باید نه به‌عنوان هزینه جاری، بلکه سـرمایه‌گذاری بلندمدت دیده شـود . (EY,2021)

جمع‌بندی تحلیلی و توصیه‌های کلیدی

حمله سایبری به بانک سپه در جنگ ۱۲ روزه اخیر، یک بیدارباش جدی برای سیستم بانکی کشور بود. این واقعه تلخ نشان داد که سیستم‌های بانکی در جنگ‌های ترکیبی نه تنها اهداف اقتصادی، بلکه اهداف استراتژیک نظامی نیز هستند. پیامدهای چنین حملاتی فراتر از خسارات مالی بوده و می‌تواند به تضعیف توان دفاعی و اعتماد ملی منجر شود. کشورهایی که امنیت سایبری را جدی نگیرند، هزینه‌های جبران‌ناپذیری خواهند پرداخت. ارتقای امنیت سایبری، تضمین پایداری اقتصادی و حفظ سرمایه اجتماعی در دنیای پرتنش امروز، ضرورتی انکارناپذیر است.

برای مقابله با این تهدیدات پیچیده، بانک‌ها باید از رویکردهای منفعل و سنتی فاصله گرفته و به سمت استقرار یک اکوسیستم سایبری مقاوم، پیش‌بین و واکنش‌گرا حرکت کنند. اجرای راهکارهای پیشنهادی، از جمله ایزولاسیون هوشمندانه شبکه‌ها، به‌روزرسانی مداوم، سرمایه‌گذاری در طرح‌های جامع تداوم کسب وکار/ بازیابی در شرایط بحرانی، بهره‌گیری از هوش سایبری و آموزش مستمر نیروی انسانی، حیاتی است. از دیدگاه حسابداری و مالی، این اقدامات نه تنها هزینه‌های بلندمدت ناشی از حملات را کاهش می‌دهند، بلکه بهبود چشمگیر در تداوم عملیات و حفظ اعتبار و اعتماد عمومی را نیز به ارمغان می‌آورند.

در یک نگاه تحلیلی:

ـ حملات سایبری می‌توانند به‌طور مستقیم سودآوری بانک‌ها را کاهش دهند.

ـ می‌توانند نسبت‌های مالی را تحت تأثیر قرار دهند.

ـ در بلندمدت هزینه سرمایه بانک را افزایش دهند.

بنابراین، بانک‌ها باید امنیت سایبری را بخشی از حاکمیت شرکتی بدانند و آن را در قالب یک نظام مدیریت ریسک جامع پیاده‌سازی کنند.

اکنون زمان اقدام پیش‌دستانه، هماهنگ و سرمایه‌گذاری استراتژیک در امنیت سایبری است. ما به عنوان متخصصان مالی، حسابداری و نرم‌افزارهای مالی، مسئولیت داریم تا با پیاده‌سازی این راهکارها، تاب‌آوری سیستم بانکی را در برابر تهدیدات سایبری تقویت کنیم و از تکرار فجایعی مانند حمله به بانک سپه جلوگیری نماییم.

فهرست منابع

Allianz Cyber Report. (2023). Global cyber insurance market outlook. Allianz Group.
BCBS. (2022). Principles for the Sound Management of Operational Risk. Bank for International Settlements.

Chertoff, M., & Simon, T. (2020). The impact of cyberattacks on financial institutions. Atlantic Council.
Cloudflare. (2022). DDoS threat landscape report. Cloudflare Inc.
Computer Emergency Response Team - Iran (CERT). (2023).
Deibert, R. (2022). Reset: Reclaiming the internet for civil society. House of Anansi.
ENISA. (2020). Cybersecurity for the finance sector. European Union Agency for Cybersecurity.
EY. (2021). Global financial services cyber survey. Ernst & Young.
FRC. (2020). Guidance on the strategic report. Financial Reporting Council.
Gopalakrishnan, S., & Trivedi, K. (2021). Cybersecurity for critical infrastructure. Springer.
IBM. (2023). Cost of a data breach report. IBM Security.
IMF. (2022). Cyber Risk and Financial Stability. International Monetary Fund.
ISO/IEC 22301. (2019). Business continuity management systems. ISO.
Kaspersky. (2023). Threat intelligence reports. Kaspersky Lab.
Microsoft Security. (2021). Modernizing banking infrastructure against cyber threats. Microsoft.
Park, S., Kim, D., & Lee, H. (2014). Cyber crisis in Korea: Lessons from major attacks. Journal of Information Security.
Putnam, R. D. (2000). Bowling alone: The collapse and revival of American community. Simon & Schuster.
PwC. (2021). The state of cybersecurity in financial services. PwC Global.
Rid, T. (2020). Active measures: The secret history of disinformation and political warfare. Farrar, Straus and Giroux.
SANS Institute. (2022). Security awareness training. SANS.
Schneier, B. (2020). Click here to kill everybody. W.W. Norton & Company.
Symantec. (2022). Cyber threats to banking systems. Symantec Enterprise.
Von Solms, R., & Van Niekerk, J. (2013). From information security to cyber security. Computers & Security, 38, 97–102.
Whitman, M. E., & Mattord, H. J. (2022). Principles of information security. Cengage Learning.
Zyskind, G., Nathan, O., & Pentland, A. (2015). Decentralizing privacy: Using blockchain to protect personal data. IEEE SPW.