APJ. 4(3):34-42, Autumn 2023

Arman Process Journal (APJ)

Homepage: armanprocessjournal.ir

Security Threats, Challenges, Procedures and Policies in Information Systems

M. Azadi[*,1]

[1] Institute of Computer science, Shahid bahonar University, Kerman, Iran

Received: 25 August 2023
Accepted: 13 November 2023

KEYWORDS:
Security,
Privacy,
Information System,
Security Policy,
Authentication,
Authorization,

[1] Corresponding author
mo.azadii@gmail.com

ABSTRACT

Nowadays, information systems as the hub of data processing and knowledge management play a vital and extensive role in digital societies. With the increasing development of technologies and the increase in the amount of information related to users and organizations, the security of information systems has become a complex and multi-dimensional challenge. In the field of security management in our information systems, we need a comprehensive understanding of all types of threats and challenges and providing approaches, policies, procedures and resources that are used to prevent security gaps, as well as protecting the system from all types of attacks affecting data and information. to be It is necessary to adopt a coherent and coordinated method to achieve the security processes of data and systems and it is necessary to understand the complexity of this category and provide comprehensive approaches based on its basic principles. Protection of information systems against unauthorized access or change to information, including storage, processing or transmission, and against denial of service to authorized users, is among the necessary measures to identify, document and deal with security threats in this area. According to the importance of the subject in this article, we will investigate the characteristics of security services of information systems in the environment of distributed networks, their importance and existing challenges, and we will express effective policies and procedures to increase security in this area.

NUMBER OF REFERENCES	NUMBER OF FIGURES	NUMBER OF TABLES
23	0	1

نشریه تخصصی آرمان پردازش، دوره ۴، شماره ۳، پاییز ۱۴۰۲

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

تهدیدات، چالش ها، رویه ها و سیاست های امنیتی در سیستم های اطلاعاتی

محمدرضا آزادی*[1]

[1] پژوهشکده علوم کامپیوتر، دانشگاه شهید باهنر، کرمان، ایران

چکیده

امروزه سیستم های اطلاعاتی به عنوان قطب پردازش داده و مدیریت دانش، در جوامع دیجیتالی نقش حیاتی و گسترده ای دارند. با توسعه روز افزون فناوری‌ها و افزایش حجم اطلاعات مرتبط با کاربران و سازمان‌ها، مساله امنیت سیستم های اطلاعاتی به یک چالش پیچیده و چند بعدی تبدیل شده است. در حوزه مدیریت امنیت در سیستم های اطلاعاتی ما نیازمند شناخت جامع انواع تهدیدات و چالش ها و ارائه رویکردها، سیاستها، رویه‌ها و منابعی که برای پیشگیری از شکافهای امنیتی مورد استفاده قرار می‌گیرند و همچنین محافظت سیستم از انواع حملات تاثیرگزار بر داده و اطلاعات، می باشیم. لازمهٔ اتخاذ یک روش منسجم و هماهنگ برای دستیابی به فرآیندهای امنیت داده‌ها و سیستم‌ها، نیازمند درک پیچیدگی این مقوله و ارائه رویکردهای جامع مبتنی بر اصول بنیادین آن است. حفاظت از سیستم های اطلاعاتی در برابر دسترسی یا تغییر غیرمجاز به اطلاعات، اعم از ذخیره، پردازش یا انتقال، و در برابر انکار سرویس به کاربران مجاز، از جمله اقدامات لازم برای شناسایی، مستندسازی و مقابله با تهدیدات امنیتی در این حوزه است. بنا به اهمیت موضوع در این مقاله، به بررسی مشخصه ها سرویس های امنیتی سیستم های اطلاعاتی در محیط شبکه های توزیعی، اهمیت آن‌ها و چالش‌های موجود می پردازیم و سیاست ها و رویه های موثر در جهت افزایش امنیت در این حوزه را بیان می نمائیم.

واژگان کلیدی:
امنیت،
حریم خصوصی،
سیستم اطلاعات،
خط مشی امنیتی،
احراز هویت،
مجوز،

تعداد جداول	تعداد شکل ها	تعداد مراجع
۱	۰	۲۳

مقدمه

امروزه حفظ امنیت سیستم های اطلاعاتی از اهمیت بسیار بالایی برخوردار است. حفاظت از سیستم های اطلاعاتی در برابر دسترسی یا تغییر غیرمجاز به اطلاعات، اعم از ذخیره، پردازش یا انتقال داده و محافظت در برابر انکار سرویس به کاربران مجاز، از جمله اقدامات لازم برای شناسایی، مستندسازی و مقابله با تهدیدات امنیتیدر این حوزه است. امنیت سیستم های اطلاعاتی، به فرآیندها و روش های مرتبط با محرمانه نگه داشتن اطلاعات، در دسترس بودن و تضمین یکپارچگی آن اشاره دارد. همچنین این موضوع به موارد زیر اشاره دارد [۲-۱]:

- کنترل های دسترسی، که از ورود یا دسترسی پرسنل غیرمجاز به یک سیستم جلوگیری می کند.
- حفاظت از اطلاعات صرف نظر از اینکه آن اطلاعات کجا هستند، یعنی در حال انتقال (مانند ایمیل) یا در یک منطقه ذخیره سازی.
- شناسایی و اصلاح نقض‌های امنیتی و همچنین مستندسازی رویدادهای مرتبط.

امروزه سیستم های اطلاعاتی به عنوان قطب ارتباطات و انتقال داده‌ها در جوامع دیجیتالی نقش حیاتی دارند. با توسعه روز افزون فناوری‌ها و افزایش حجم اطلاعات مرتبط با کاربران و سازمان‌ها، امنیت سیستم های اطلاعاتی به یک چالش پیچیده تبدیل شده است. اخیرا تهدیدات امنیتی به یک خطر مشترک و همگانی در حوزه سیستم های اطلاعاتی تبدیل شده اند شده‌اند. لذا، استراتژی های مدیریتی و سیاستهای امنیتی سازمان ها باید به این موضوع حیاتی بیش از پیش توجه نموده و روش‌های مقابله با این چالش ها را ارائه نمایند. اصولاً اگر به هنگام نیاز، اطلاعات ذخیره و پردازش شده به وسیلهٔ یک سیستم اطلاعاتی در دسترس نباشد، چنین سیستمی استفاده‌ای ندارد. تهدیدات زیادی بر علیه امنیت و قابلیت دسترسی به داده‌ها وجود دارد که بسیاری از آن‌ها ویژه محیط کامپیوترهای شخصی است. در حالی که افراد به مسایل سرقت کامپیوترهای بزرگ و داده‌های آن به عنوان یک تهدید جدی به نسبت توجه دارند، این موضوع در مورد انواع سیستم های اطلاعاتی توزیعی بسیار بیشتر اتفاق می‌افتد ولی کمتر مورد توجه است. صحت و درستی اطلاعات یک سیستم اطلاعاتی یکی از ملاحظات مهم امنیتی آن سیستم است. ارزش هر تصمیم‌گیری وابسته به کیفیت اطلاعاتی است که از سیستم اطلاعاتی دریافت می‌شود. از جمله برای افزایش اطمینان، باید از نرم‌افزارهای مجاز بر روی سیستم استفاده کرد. زیرا بعضی از ویروس‌هایی که در اثر استفاده از اجرای غیرمجاز برنامه‌ها شایع می‌شوند به جای تخریب کامل اطلاعات تنها بخشی از آن را تغییر می‌دهند. بر این اساس ممکن است کاربر پس از این که در یک موقعیت حساس تصمیماتی را بر اساس چنین اطلاعاتی گرفته باشد، متوجه بروز خطا و تغییر داده‌ها شود. خطر دیگر، امکان دست کاری اطلاعات به وسیلهٔ کارکنان یک سازمان است، در این صورت نیز هیچ گونه اطمینانی از صحت اطلاعات ذخیره شده وجود نخواهد داشت [۳]. یک مساله دیگر در ارتباط با صحت اطلاعات، نرم‌افزارهایی است که بعضاً به کمک سیستم های اطلاعاتی آماده می‌شوند. افراد در محیط کامپیوترهای شخصی می‌توانند نرم‌افزارهایی را خیلی سریع و بدون انجام تست‌های کافی تهیه کنند، بدون توجه به این که این نرم‌افزار ممکن است بعداً به عنوان جزئی از یک نرم‌افزار بزرگ‌تر مورد استفاده قرار گیرد. عدم دقت کافی در آزمایش نرم‌افزار و تهیه مستندات ممکن است هر روز اشکالاتی ایجاد کند. برای تهدیدات بر علیه امنیت پردازش الکترونیکی داده‌ها می‌توان این تعریف را ارایه داد: «هرگونه عمل یا اتفاقی که به طور خلاف بر امنیت پردازش الکترونیکی داده‌ها تاثیر گذارند» [۴].

محرمانه بودن اغلب شرط لازم و اولیه امنیت داده‌ها است که به وسیلهٔ کاربران به آن اشاره می‌شود. در کار روزانه افراد معمولاً در حفظ اسناد، طبقه‌بندی کردن آن‌ها و قفل کردن قفسه‌ها توجه کافی دارند. در حالی که در مورد نگهداری داده‌ها در سیستم کامپیوتری چنین حساسیتی کمتر به چشم می‌خورد. با توجه به موارد ذکر شده اهمیت دادن به مقوله امنیت داده‌ها و سیستم‌ها تا حدودی افزایش یافته است. به طور خلاصه پاره‌ای از دلایل اهمیت و ضرورت مساله امنیت داده‌ها در سیستم های اطلاعاتی را در موارد زیر می‌توان خلاصه کرد [۶-۵]:

ـــ خدشه‌پذیری سیستم‌ها به خاطر اشتیاق پاره‌ای از متخصصان به شکستن موانع امنیتی و نفوذ به درون سیستم‌های کامپیوتری

ـــ هراس از بین رفتن کنترل مدیریت بر روی اطلاعات

ـــ تغییر شکل در ماهیت اطلاعات تراکنش های اداری و مالی

ـــ افزایش حجم فرایندهای تجاری و مبادلات پولی که به صورت الکترونیکی مبادله می‌شود

ـــ افزایش و وجوه انگیزه برای ارتکاب جرایم کامپیوتری

ـــ طرح قوانین مرتبط با فن‌آوری کامپیوتر و لزوم پیروی از آن‌ها

ـــ جالب بودن جنبهٔ رسانه‌ای کامپیوتر و دریافت اطلاعات از این طریق

ـــ وجود آسیب زنندگان و افراد غیر مجاز که وارد شبکه می‌شوند

ـــ شایع بودن و فراگیری روزافزون بدافزارها و ویروس‌های کامپیوتری

ـــ لزوم توجه به تجزیه و تحلیل خطرات ناشی از بروز اتفاقات

در مقابل ضرورت امنیت سیستم‌ها، پاره‌ای از نتایج حاصل از عدم ایجاد امنیت در عرصهٔ داده‌ها و کاربردهای مختلف سیستم‌های اطلاعاتی وکامپیوتری را می‌توان چنین برشمرد [۷]:

ـــ شکست فعالیت‌های کاری برنامه‌ریزی شده

ـــ از دست دادن اطلاعات مهم و دارایی‌ها و بروز زیان‌های مالی

ـــ غیر قابل اعتماد شدن سیستم‌ها

ـــ از دست دادن مشتریان یا نارضایتی آنها

ـــ شکست در عرضه خدمات قابل قبول

ماهیت امنیت داده‌ها و سیستم‌ها

امنیت دارای یک مفهوم گسترده و در عین حال انتزاعی با ویژگی‌های خاص خود است. تمرکز امنیت بر روی تهدیدات و حملات به عمل آمده بر علیه سیستم‌های اطلاعاتی، تشخیص انجام و نوع این تهدیدات، نحوهٔ جلوگیری و چگونگی بازگشت به شرایط نرمال کارکرد سیستم است.

لازمهٔ اتخاذ یک روش منسجم و هماهنگ برای دستیابی به فرآیندهای امنیت داده‌ها و سیستم‌ها، نیازمند درک پیچیدگی این مقوله و بالاخره مبتنی بر اصول بنیادین آن (به طوری که ما را به یک طرح اجرایی رهنمون سازد) است. به طور کلی سیستم‌های امن با استفاده از ویژگی‌های مشخص امنیتی، دستیابی به اطلاعات را چنان کنترل می‌کنند که فقط اشخاص مجاز و یا پردازش‌هایی که از جانب آن‌ها ایجاد می‌شود، مجاز به انجام عملیات خواندن، نوشتن، ایجاد و یا حذف اطلاعات باشند. بنا به اهمیت موضوع در این مقاله، به بررسی مشخصه ها سرویس های امنیتی سیستم های اطلاعاتی در محیط شبکه های توزیعی، اهمیت آن‌ها، چالش‌های موجود و راهکارهای افزایش امنیت در این حوزه خواهیم پرداخت.

تهدیدات و چالش های امنیتی

تهدیدات امنیتی سیستم های اطلاعاتی، خطرات احتمالی هستند که احتمالاً می توانند عملکرد عادی چنین سیستم هائی را مختل کنند و اطلاعات نادرست را وارد چرخه پردازش اطلاعات و سیستم های داده کاوی نمایند. در عصر حاضر، با دیجیتال شدن جهان، چنین تهدیداتی به طور مداوم در حال افزایش است. تهدیدات پایه امنیتی در سیستم های اطلاعاتی و کامپیوتری عبارتند از [۹-۸]:

ویروس های کامپیوتری

ویروس کامپیوتری یک برنامه مخرب است که بدون اطلاع کاربر در رایانه کاربر بارگذاری می شود. خود را تکرار می کند و فایل ها و برنامه های رایانه شخصی کاربر را آلوده می کند. هدف نهایی یک ویروس این است که اطمینان حاصل شود که رایانه قربانی هرگز نمی تواند به درستی یا حتی اصلاً کار کند. همچنین کرم کامپیوتری یک برنامه نرم افزاری است که می تواند خود را از یک کامپیوتر به کامپیوتر دیگر بدون تعامل انسانی کپی کند. خطر بالقوه در اینجا این است که فضای دیسک سیستم اطلاعاتی را مصرف می کند زیرا یک کرم می تواند با حجم زیاد و با سرعت زیاد تکثیر شود.

حملات فیشینگ

فیشرها که به عنوان یک شخص یا کسب و کار قابل اعتماد ظاهر می شوند، سعی می کنند اطلاعات مالی یا شخصی حساس را از طریق ایمیل های جعلی یا پیام های فوری سرقت کنند. متأسفانه اجرای فیشینگ بسیار آسان است. شما فریب خورده اید که فکر می کنید این نامه قانونی است و ممکن است اطلاعات شخصی خود را وارد کنید.

بات نت

بات نت گروهی از رایانه های متصل به اینترنت است که توسط یک هکر با استفاده از یک ویروس رایانه ای در معرض خطر قرار گرفته اند. به یک رایانه شخصی «رایانه زامبی» می گویند. نتیجه این تهدید رایانه قربانی است که ربات برای فعالیت های مخرب و برای حمله در مقیاس بزرگتر مانند DDoS استفاده می شود.

حملات روت کیت

روت کیت یک برنامه کامپیوتری است که برای فراهم کردن دسترسی ممتاز مستمر به یک کامپیوتر در حالی که فعالانه حضور آن را پنهان می کند طراحی شده است. هنگامی که یک روت کیت نصب شد، کنترلر روت کیت قادر خواهد بود فایل ها را از راه دور اجرا کند و پیکربندی های سیستم را در سیستم میزبان تغییر دهد و درکار سیستم اطلاعاتی و رایانه ای اختلال ایجاد نماید.

کی لاگر

کی لاگر که به عنوان Logger ضربه زدن به کلید شناخته می شود، می تواند فعالیت بلادرنگ کاربر را در رایانه خود ردیابی کند. کی لاگر یک رکورد از تمام ضربه های کلید ساخته شده توسط صفحه کلید کاربر را نگه می دارد Keylogger .همچنین یک تهدید بسیار قدرتمند برای سرقت اطلاعات اعتبار ورود افراد مانند نام کاربری و رمز عبور است.

همچنین از سایر تهدیدات سطح بالایی که پیرامون سیستم های اطلاعاتی در محیط سیستم های توزیعی قابل تعریف است، به موارد زیر می‌توان اشاره کرد [۱۲-۱۰]:

- جمع‌آوری اطلاعات (Information gathering)
- شنود و استراق سمع (Sniffing & Eavesdropping)
- جعل (Spoofing)
- روبایش نشست‌ها (Session hijacking)
- حمله مرد میانی (Man-in-the-Middle Attack)
- مسوم‌سازی DNS و ARP (DNS & ARP Poisoning)
- حملات مبتنی بر گذرواژه (Password-based Attacks)
- حملات انکار سرویس (Denial-of-Services Attacks)
- حملات روبایش کلید (Compromised Key Attacks)
- حملات دیوارآتش و تشخیص نفوذ (Firewall&IDS Attacks)

لازم به ذکر است،درون ساختار سیستم های اطلاعاتی اطلاعات مشابه هر موجودیت فیزیکی می‌تواند تغییر کرده، از بین برود و یا از کنترل صاحب آن خارج شود. اما بر خلاف موجودیت‌های فیزیکی و بدون این که اثری از فعالیت انجام شده باقی بماند، اطلاعات می‌تواند کپی شده و یا به طور ناخودآگاه شنیده شود. بهای دستیابی به کپی یا استراق سمع اطلاعات در مقایسه با ارزش واقعی آن، بسیار ناچیز است. همچنین درحالت عمومی تهدیدات امنیتی سیستم های اطلاعاتی به دو رده سهوی و عمدی قابل تقسیم می باشند. چالش های امنیتی سیستم های کامپیوتری یا احتمال به خطر افتادن امنیت اطلاعات را می‌توان به سه رده کلی تقسیم کرد [۱۳]:

- عدم دسترسی یا امتناع از ارایه خدمات (اطلاعات به هنگام نیاز قابل دسترسی نیست).
- عدم درستی و صحت اطلاعات (تغییر و یا تخریب اطلاعات)

- غیر قابل اطمینان بودن اطلاعات (به وسیلهٔ اشخاص غیر مجاز کپی، دیده و یا شنیده شوند).

چه بسا مبنای این خطرات خصوصاً موارد اول و دوم بدخواهانه نباشد بلکه می‌تواند به صورت حادثه و اتفاقی باشند. برای مثال خرابی ناشی از سیل یا آتش‌سوزی می‌تواند دلایلی برای عدم قابلیت دسترسی به اطلاعات باشند، اگر چه نتیجه چنین خطرهایی با وجود دلایل مختلف یکسان خواهد بود. احتمال بیشتر بروز پاره‌ای از خطرها نسبت به بعضی دیگر، وابسته به شرایط خاص هر سیستم و محل آن است. بنابراین سیاست امنیتی باید مشخص کند که روی چه مواردی باید تاکید کرد. در تجزیه و تحلیل خطرها چنین به نظر می‌رسد که باید خطرها را بر اساس این که چگونه به وجود می‌آیند تقسیم بندی کرد. زیرا بدین طریق پیش‌بینی تناوب و تواتر بروز خطرات ممکن آسان‌تر خواهد بود. در جدول زیر یک دسته‌بندی کلی از تهدیدات عمدی و سهوی این حوزه ارائه شده است [۱۵-۱۴]:

جدول۱.طبقه بندی انواع زمینه های تهدیدات امنیتی

زمینه تهدیدات	امنیت فیزیکی	امنیت داده‌ها
سهوی	حوادث جزیی، بلایای طبیعی	خطاهای برنامه و مسایل ناشی از عملیات
عمدی	جنگ، خرابکاری، تخریب	کلاهبرداری، خرابکاری، دزدی و درز کردن اطلاعات محرمانه

تهدیدات بر علیه امنیت فیزیکی شامل خطرهایی است که ساختمان، سخت‌افزار، سایت کامپیوتری، خطوط انتقال داده و منابع تغذیه را تهدید می‌کند. حوادث و تهدیداتی که بر امنیت فیزیکی تاثیر می‌گذارند به دو دسته حوادث غیر عمدی و عمدی تقسیم می‌شود:

- حوادث غیرعمدی از کوچک‌ترین خطاها در مسایل تکنیکی تا عظیم‌ترین بلایای طبیعی را شامل می‌شود. از این قبیل حوادث، آتش سوزی، سیل، زلزله، رطوبت، گرما یا سرمای شدید، خطاهای سخت‌افزار، نقص منبع تغذیه قابل ذکر است.
- حوادث عمدی هر حادثه‌ای از قبیل جنگ و خرابکاری در تجهیزات، سرقت حافظه‌های جنبی محتوی پرونده‌های اطلاعاتی، ورود غیرمجاز به نواحی حفاظت شده و یا اشکالاتی که به ندرت ممکن است در سیستم‌های کامپیوتری بروز کند، را شامل می‌شود. حفاظت بر علیه این نوع تهدیدات نیز عمدتاً همان روش‌های حفاظتی که بر علیه حوادث و تهدیدات غیر عمدی باید صورت پذیرد، خواهد بود.

از سوی دیگر، عموماً یک متجاوز می‌تواند به هر نقطه‌ای از شبکه بصورت فعال[1] یا غیر فعال[2] حمله نماید. در یک حملهٔ غیر فعال متجاوز صرفاً اطلاعات عبوری از میان کانالهای سیستم را بدون دخالت در جریان یا محتویاتشان مشاهده می‌نماید. این نوع بنام حملهٔ آگاهی از محتویات پیام[3] نامیده شده و نمونه‌ای از یک حملهٔ غیرفعال است. متجاوز ممکن است با بدست آوردن موقعیت و هویت طرفین ارتباط و آگاهی از طول و فرکانس پیامهای عبوری از کانال تجزیه و تحلیل ترافیک را انجام دهد هر چند که این اطلاعات برای او غیر قابل درک باشد. در یک تجاوز یا حملهٔ فعال، متجاوز بر روی اطلاعات مبادله شده اثر می‌گذارد. او می‌تواند تغییر، تکرار، درج پیام معتبر و یا غیر معتبر، حذف، تاخیر، و یا تغییر ترتیب پیامها را در یک یا هر دو مسیر (جهت) کانال ارتباطی انجام دهد. این حملات به عنوان حملات تغییر دنبالهٔ پیام[4] نامیده می‌شوند متجاوز ممکن است تمام پیام را حذف و یا به تاخیر اندازد، که بنام حملات تکذیب سرویس پیام شناخته می‌شوند. این نوع حملات با فرض برقراری ارتباط بین دو جزء انجام میشود، در ابتدا اتصال بین طرفین باید بروش امنی برقرار گردد که این مسئله با بررسی هویت طرفین اتصال و درستی زمان اتصال تحقق مییابد. حمله در برابر برقراری اتصال اولیه شامل تکرار همین مراحل آماده‌سازی می‌باشد. این نوع از حملات اتصال اولیه جعلی نامیده می شود. عموماً حملات غیرفعال آشکار و کشف نمی‌گردند اما می‌توان به آسانی از آنها جلوگیری نمود. در حالی که حملات فعال به آسانی کشف می‌گردند اما نمی‌توان از آنها جلوگیری کرد [۱۶].

در حوزه مدیریت امنیت در سیستم های اطلاعاتی ما نیازمند رویکردهائی همانند سیاستها و رویه‌ها، منابعی که برای پیشگیری از شکافهای امنیتی مورد استفاده قرار می‌گیرند و محافظت سیستم از انواع حملات تاثیرگزار بر داده و اطلاعات می باشیم.

رویه‌ها و سیاستهای امنیتی

بمنظور چاره اندیشی امنیتی و برای جلوگیری از دسترسی غیرمجاز به داده‌ها در مراکز داده و سیستمهای اطلاعاتی مرتبط، می‌توان از راهکارهای زیر استفاده کرد [۱۸-۱۷]:

[1] active
[2] passive
[3] message coatent learning attack
[4] -messaje stream modificatiom attrcks

تامین امنیت فیزیکی

ایجاد امنیت فیزیکی قوی در مراکز داده و سیستمهای اطلاعاتی مرتبط بسیار مهم است. این موضوع شامل استفاده از سیستم‌های کنترل دسترسی فیزیکی مانند قفل‌ها، دوربین‌های مداربسته، سیستم‌های اعلام سرقت و سایر تجهیزات امنیتی است. همچنین، محدود کردن دسترسی فیزیکی برای افراد مجاز و نظارت دقیق بر ورود و خروج افراد از مرکز داده می‌تواند کمک کند.

رمزنگاری داده‌ها

استفاده از پروتکل های رمزنگاری برای محافظت از داده‌ها در طول انتقال و در حالت ذخیره‌سازی بسیار حائز اهمیت است. با استفاده از الگوریتم‌های رمزنگاری قوی مانند AES [1] می‌توان از داده‌ها حتی در صورت دسترسی غیرمجاز به آن‌ها محافظت کرد.

تامین امنیت شبکه

ایجاد سیستم‌های امنیتی قوی برای شبکه مرکز داده و سیستمهای اطلاعاتی از اهمیت بالایی برخوردار است. این موضع شامل استفاده از دیوارهای آتش، روترهای پیشرفته و سطح بالا، به کارگیری سیستم‌های تشخیص نفوذ و مدیریت دسترسی به شبکه است .همچنین، باید به‌روزرسانی نرم‌افزارها و وصله‌های امنیتی در چک لیست شبکه قرار بگیرد تا ضعف‌های امنیتی را پوشش دهند.

مدیریت هویت و دسترسی

به کارگیری سیستم مدیریت هویت و دسترسی قوی در مرکز داده می‌تواند کمک کند تا فقط افراد مجاز به داده‌ها دسترسی پیدا کنند. این موضوع شامل استفاده از روش‌های احراز هویت قوی مانند احراز هویت دو عاملی ، استفاده از سیستم‌های سندباکس و تعیین سطوح دسترسی بر اساس نیازهای کاربران است.

نظارت و آموزش

نظارت مداوم بر سیستم‌ها و فعالیت‌های مرکز داده می‌تواند به تشخیص و پاسخ‌دهی زودهنگام به هر نوع دسترسی غیرمجاز کمک کند. همچنین، آموزش کارکنان درباره بهترین شیوه‌های امنیتی و آگاهی از تهدیدات روزصفر نقش مهمی در کم کردن شانس هکرها برای نفوذ به مراکز داده دارد.

همچنین برای تامین و تضمین امنیت سیستمهای اطلاعاتی باید بر مبنای مراحل مختلفی گام بردارید. این موضوع به نوع مرکز داده، تجهیزات نصب شده در آن و اطلاعاتی که میزبانی می‌کند، بستگی دارد. با این‌حال، برخی از این روش‌ها به شرح زیر هستند [۱۹]:

طراحی و پیاده‌سازی بر مبنای یک معماری ایمن

امنیت باید از مرحله طراحی و برنامه‌ریزی مراکز داده در نظر گرفته شود. ایجاد یک زیرساخت و معماری امن با در نظر گرفتن مکان‌های فیزیکی، شبکه‌ها، سیستم‌ها و راهکارهای امنیتی مانند جدا کردن شبکه‌ها، ایجاد لایه‌های امنیتی و کنترل دسترسی می‌تواند امنیت مراکز داده را تضمین کند.

استفاده از تجهیزات و فناوری‌های امنیتی

استفاده از تجهیزات و فناوری‌های امنیتی مانند دیوارهای آتش، سیستم‌های تشخیص نفوذ، رمزگذاری داده، کنترل دسترسی فیزیکی و دیگر تجهیزات امنیتی می‌تواند به حفاظت از مراکز داده و سیستم های اطلاعاتی مرتبط کمک کند. این تجهیزات باید به‌روزرسانی و مدیریت شوند تا بهترین سطح امنیت را فراهم کنند.

مدیریت نقش‌ها و حساب‌های کاربری

استفاده از سیستم‌های مدیریت هویت و دسترسی اجازه می‌دهد کنترل دقیقی بر روی دسترسی کاربران به داده‌ها و سیستم‌ها داشته باشید. احراز هویت قوی، تعیین سطوح دسترسی مبتنی بر نقش و مسئولیت، تعیین سطوح دسترسی به اطلاعات حساس و محدود کردن دسترسی به حداقل لازم از جمله اقدامات ضروری و مهمی است که می‌تواند امنیت را تضمین کند [۲۰].

پشتیبانی و به روزرسانی مداوم

نرم‌افزارها و سیستم‌ها در مراکز داده باید به روزرسانی شوند و پچ‌های امنیتی جدید نصب شوند. همچنین، باید روش‌های پشتیبانی و بازیابی داده موثر و قابل اعتماد در مرکز داده وجود داشته باشد تا در صورت وقوع حادثه‌های امنیتی، داده‌ها قابل بازیابی باشند.

فرهنگ سازی، آموزش و آگاهی

فرهنگ سازی و آموزش کارکنان درباره بهترین شیوه‌های امنیتی، تشخیص تهدیدات و رفتارهای مشکوک و آگاهی از خطرات امنیتی می‌تواند در جلوگیری از دسترسی غیرمجاز به داده‌ها و تضمین امنیت مراکز داده موثر باشد. کارکنان باید به طور منظم آموزش‌های امنیتی دریافت کنند و آگاهی داشته باشند که چگونه با تهدیدات امنیتی برخورد کنند و رفتارهای امنیتی را رعایت کنند.

رصد و ارزیابی امنیتی منظم

ارزیابی‌های امنیتی منظم بر روی مراکز داده و سیستم‌های اطلاعاتی باید بصورت مستمر و منظم انجام شود. این موضوع شامل آزمون نفوذ، آزمون امنیتی، بررسی آسیب‌پذیری‌ها و ارزیابی عملکرد امنیتی است. با

[1] Advanced Encryption Standard (AES)

انجام ارزیابی‌های منظم، ضعف‌های امنیتی شناسایی و بهبودهای لازم و موردنیاز اعمال می‌شود.

رعایت قوانین و مقررات

رعایت قوانین و مقررات امنیتی مرتبط با حوزه مراکز داده بسیار حایز اهمیت است. باید با قوانین حریم خصوصی، حفاظت از داده‌ها و سایر قوانین مرتبط آشنا بوده و آن‌ها را رعایت کرد.

استفاده همزمان از این راهکارها و بهره گیری از یک معماری‌های امنیتی مناسب می‌تواند به تضمین امنیت مراکز داده و سیستم های اطلاعاتی مرتبط کمک کند. همچنین، مهم است که به‌روزرسانی‌ها و تحولات جدید در حوزه امنیت بررسی شوند تا با تهدیدات امنیتی روزمره مراکز داده به درستی مقابله گردد. همچنین برای مدیریت هویت و دسترسی به داده‌ها، می‌توان از راهکارها و تکنیک‌های زیر استفاده کرد:

احراز هویت چند عاملی

در این روش، برای احراز هویت یک کاربر، از ترکیب چندین عامل استفاده می‌شود. عامل‌های قابل استفاده شامل رمز عبور، کارت هوشمند، اثر انگشت، تشخیص چهره و دیگر ویژگی‌های زیستی هستند. این روش احراز هویت قوی‌تری را فراهم می‌کند و از حملات مبتنی بر رمزگشایی یا دسترسی غیرمجاز محافظت می‌کند [۲۱].

سیستم‌های تشخیص نقش و مسئولیت

با استفاده از سیستم‌های تشخیص نقش و مسئولیت(RBAC) ، سطوح دسترسی کاربران بر اساس نقش و مسئولیت‌های آن‌ها تعیین می‌شود. این سیستم مشخص می‌کند که هر کاربر در سازمان چه دسترسی‌هایی به داده‌ها و سیستم‌ها دارد و به این ترتیب حق دسترسی به داده‌ها به صورت مبتنی بر نقش تعیین می‌شود.

مدیریت هویت و دسترسی بر پایه سرویس

این راهکار شامل استفاده از سیستم‌ها و فرآیندهای مربوط به مدیریت هویت و دسترسی است که به کنترل دسترسی به منابع در سطح سازمان کمک می‌کند. با استفاده از این سیستم، مدیران می‌توانند هویت کاربران را مدیریت کنند، سطوح دسترسی را تعیین کنند و کنترل دقیقی بر روی دسترسی به داده‌ها و سیستم‌ها داشته باشند.

اصل حداقل دسترسی

اصل حداقل دسترسی به این معنی است که هر کاربر فقط دسترسی لازم را برای انجام وظایف خود دریافت کند و دسترسی به منابع دیگری که برای انجام وظایفش لازم نیست، نداشته باشد. این روش کمک می‌کند تا ریسک‌های امنیتی کاهش یابد و احتمال دسترسی غیرمجاز کاربران به داده‌ها کاهش یابد.

تعیین سطوح دسترسی بر اساس محتوا

با استفاده از تکنیک‌هایی مانند برچسب‌گذاری داده‌ها و طبقه‌بندی محتوا می‌توانید سطوح دسترسی کاربران را بر اساس محتوای داده‌ها تعیین کنید. در این روش، هر داده برچسبی مشخص دریافت می‌کند و سطح دسترسی کاربران مختلف بر اساس این برچسب‌ها تعیین می‌شود. به این ترتیب، کاربران فقط به داده‌هایی دسترسی دارند که برای آن‌ها مجاز شده‌اند.

غیرقابل خواندن کردن داده‌ها در حالت عادی

استفاده از رمزنگاری برای حفاظت از داده‌ها در حالت استفاده نشده و در حال انتقال بین سیستم‌ها می‌تواند امنیت دسترسی به داده‌ها را افزایش دهد. با رمزنگاری داده‌ها، حتی اگر همگان به داده‌ها دسترسی داشته باشند، فقط افرادی که دارای کلید رمزنگاری هستند می‌توانند آن‌ها را خوانده یا بازیابی کنند.

مانیتورینگ و ثبت وقایع

سیستم‌های مانیتورینگ و ثبت وقایع می‌توانند به شناسایی و پی‌گیری فعالیت‌های کاربران در سیستم‌ها کمک کنند. با نظارت بر رویدادها و ثبت آن‌ها، می‌توانید به سرعت هرگونه فعالیت غیرمجاز یا نامناسب در دسترسی به داده‌ها و سیستم‌ها را شناسایی کنید.

مدیریت چرخه عمر

با مدیریت چرخه عمر هویت کاربران و دسترسی‌ها، می‌توانید در زمان لازم دسترسی کاربران را تغییر دهید یا لغو کنید. به عنوان مثال، هویت کاربرانی که از سازمان خارج شده‌اند، می‌تواند غیرفعال شده و دسترسی آن‌ها به داده‌ها قطع شود.

جلوگیری از خطای انسانی

خطای انسانی یک نقطه ضعف بزرگ است که به راحتی توسط مجرمان سایبری مورد سوء استفاده قرار می گیرد. کاربران نهایی در حال تبدیل شدن به بزرگترین خطر امنیتی در هر سازمانی هستند. با این حال، کاربر نهایی هیچ تقصیری از خود ندارد و بیشتر به دلیل عدم آگاهی و سیاست ICT است. آنها می توانند ناخواسته دروازه های مجازی را به روی مهاجمان سایبری باز کنند. به همین دلیل است که سیاست‌ها، رویه‌ها و پروتکل‌های امنیتی جامع باید توسط کاربرانی که به اطلاعات حساس سیستمهای اطلاعاتی دسترسی دارند، عمیقاً درک شوند. بهتر است برنامه آموزشی آگاهی امنیتی به آنها ارائه شود [۲۲].

تهدیدات امنیتی در سیستم های اطلاعاتی اخیرا به طور بی امان مبتکرانه شده اند. برای محافظت در برابر این تهدیدات پیچیده و فزاینده امنیتی رایانه ای و حفظ امنیت آنلاین، نیاز زیادی وجود دارد که فرد خود را با اطلاعات و منابع مسلح کند. هر کدام از انواع این حملات به نوبه خود می‌توانند موجب افشا، تخریب، دستکاری و دسترسی غیرمجاز به اطلاعات سازمانی و متعاقب آن از بین رفتن اعتبار سازمان شوند.

متخصصین حوزه امنیت در سیستم های اطلاعاتی بر این باورند که جهت مقابله با تهدیدات بررسی شده در مقاله حاضر، می‌توان از راه‌کارهای کلی زیر نیز بهره جست [۲۳]:

- پویش آسیب‌پذیری شبکه
- تهیه طرح جامع امنیت سیستم اطلاعاتی در سازمان
- ایمن‌سازی زیرساخت شبکه
- برنامه ریزی مدون جهت بروزرسانی و نصب وصله‌های امنیتی
- تدوین مستند الزامات و رویه های کنترل دسترسی و نیز بررسی نیازمندی ها و الزامات
- رصد دائمی شبکه و طراحی ساختار آنالیز وقایع شبکه جهت جلوگیری از بروز رخدادها
- برگزاری مانورهای ارزیابی امنیتی در سیستمهای اطلاعاتی
- تدوین نقشه راه بروزرسانی تجهیزات سازمانی و عدم استفاده از تجهیزات فاقد پشتیبانی از سوی ارائه دهندگان
- استفاده از تجهیزات حفاظتی سخت افزاری با تنظیمات دقیق و مناسب مانند دیوار آتش و WAF و...
- استفاده از سامانه های نرم‌افزاری حفاظتی مانند آنتی ویروس، RASP و...

نتایج حاصل از ایمن‌سازی سیستم های اطلاعاتی در سازمان های مختلف می‌تواند موجب ایجاد ارزش افزوده برای سازمان ها در ابعاد صحت و کارائی سیستم ها، ابعاد اجرائی، مالی و اعتباری گردد. همچنین بهره‌وری در زمان و عملکرد بستر ارتباطی سازمان یکی دیگر از ابعاد این رویکرد ایمن سازی به شمار می‌رود.

منابع و مآخذ

[1] Hernes M, Rot A, Jelonek D, editors. Towards Industry 4.0: Current Challenges in Information Systems. Cham, Switzerland: Springer; 2020 Mar 10.

[2] Wolf W, White GB, Fisch EA, Crago SP, Pooch UW, McMahon JO, Yeung D, Nguyen H, Arakawa M, MacDonald T, Akgul BE. Computer system and network security. CRC press; 2017 Dec 14.

[3] Usmonov M. BASIC CONCEPTS OF INFORMATION SECURITY IN INFORMATION SYSTEMS. WIDE THREATS AND THEIR CONSEQUENCES. Scienceweb academic papers collection. 2021 Jan 1.

[4] Carroll JM. Computer security. Butterworth-Heinemann; 2014 May 20.

نتیجه‌گیری

امروزه امنیت مراکز داده و سیستم های اطلاعاتی به عنوان یک چالش اساسی در دنیای دیجیتالی مورد توجه قرار گرفته است. تهدیدات امنیتی در سیستم های اطلاعاتی اخیرا به طور بی امان مبتکرانه شده اند. برای محافظت در برابر این تهدیدات پیچیده و فزاینده امنیتی رایانه ای و حفظ امنیت آنلاین، نیاز زیادی وجود دارد که فرد خود را با اطلاعات و منابع مسلح کند. هر کدام از انواع این حملات به نوبه خود می‌توانند موجب افشا، تخریب، دستکاری و دسترسی غیرمجاز به اطلاعات سازمانی و متعاقب آن از بین رفتن اعتبار سازمان شوند. با توجه به اهمیت این سیستم ها در پردازش و انتقال اطلاعات و داده‌ها در چرخه حیات سیستم و سازمان، شناخت انواع تهدیدات و چالش های امنیتی متصور بر این سیستم ها و همچنین چاره اندیشی درخصوص سیاست ها و رویه های مقابله با این تهدیدات از اهمیت ویژه ای برخوردار است. لذا با توجه به ضرورت پژوهش در این حوزه، این موضوع محور تحقیق در پژوهش حاضر بوده است. در این مقاله پس از بررسی چالش ها و تهدیدات امنیتی رایج در مراکز داده و سیستم های اطلاعاتی، رویه های امنیتی و سیاست گزاری های موثر در جهت مقابله با چالش های ذکر شده را بررسی نمودیم.

تعارض منافع

«هیچ‌گونه تعارض منافع توسط نویسندگان بیان نشده است»

[5] Jouini M, Rabai LB, Aissa AB. Classification of security threats in information systems. Procedia Computer Science. 2014 Jan 1;32:489-96.

[6] Stallings W. Computer security principles and practice. 2015.

[7] Ruiz Ben E, Scholl M. The Concept of Usable Privacy and Information Security. InUsable Privacy and Security in Online Public Services 2023 Nov 4 (pp. 1-12). Cham: Springer Nature Switzerland.

[8] Awan JH, Memon S, Khan RA, Noonari AQ, Hussain Z, Usman M. Security strategies to overcome cyber measures, factors and barriers. Eng. Sci. Technol. Int. Res. J. 2017;1(1):51-8.

[9] Elmaghraby AS, Losavio MM. Cyber security challenges in Smart Cities: Safety, security

and privacy. Journal of advanced research. 2014 Jul 1;5(4):491-7.

[10] Serpanos DN, Voyiatzis AG. Security challenges in embedded systems. ACM Transactions on embedded computing systems (TECS). 2013 Mar 29;12(1s):1-0.

[11] Levitin G, Hausken K, Taboada HA, Coit DW. Data survivability vs. security in information systems. Reliability Engineering & System Safety. 2012 Apr 1;100:19-27.

[12] Buccafurri F, Holzinger A, Kieseberg P, Tjoa M, Weippl E. Availability, Reliability, and Security in Information Systems. Springer International Publishing; 2016.

[13] Teufel S, Min T, You I, Weippl E. Availability, reliability, and security in information systems. Springer; 2014.

[14] Jürjens J, Rosado DG, Sánchez LE, Fernández-Medina E. Security in information systems: New challenges and opportunities.

[15] Chen F. An investigation and evaluation of risk assessment methods in Information systems.

[16] Rosado DG, Sánchez LE, Fernández-Medina E, Jürjens J. Security in Information Systems: New Challenges and Opportunities J. UCS Special Issue. Journal of Universal Computer Science. 2012 Jan 1;18(6):728-31.

[17] Hnatiienko H, Babenko T, Kovalova Y, Myrutenko L. Method of Early Detection of Information Security Anomalies and Incidents in Information Systems.

[18] Arogundade OT, Abayomi-Alli A, Misra S. An ontology-based security risk management model for information systems. Arabian Journal for Science and Engineering. 2020 Aug;45:6183-98.

[19] Gunduz MZ, Das R. Cyber-security on smart grid: Threats and potential solutions. Computer networks. 2020 Mar 14;169:107094.

[20] Berdik D, Otoum S, Schmidt N, Porter D, Jararweh Y. A survey on blockchain for information systems management and security. Information Processing & Management. 2021 Jan 1;58(1):102397.

[21] Vangala A, Das AK, Chamola V, Korotaev V, Rodrigues JJ. Security in IoT-enabled smart agriculture: Architecture, security solutions and challenges. Cluster Computing. 2023 Apr;26(2):879-902.

[22] Liang X, Kim Y. A survey on security attacks and solutions in the IoT network. In2021 IEEE 11th annual computing and communication workshop and conference (CCWC) 2021 Jan 27 (pp. 0853-0859). IEEE.

[23] Breda G, Kiss M. Overview of information security standards in the field of special protected industry 4.0 areas & industrial security. Procedia Manufacturing. 2020 Jan 1;46:580-90.