امنیت الکترونیک

فصل‌نامهٔ تخصصی، علمی، آموزشی و خبری صنعت امنیت الکترونیکی (e-security)

سال پنجم | شمارهٔ پنجم | زمستان ۱۴۰۲ | ۲۰۰ هزار تومان

در این شماره می‌خوانیم:


هزاربین
آتن
آزمایشگاه تجهیزات نظارت تصویری
سیمنا
سامانه یکپارچه مدیریت و نظارت ایکس-ری
Automation
IP
سامانه
میهن
سامانه مدیریت یکپارچه هشدار نفوذ
رخ پایش
نگهبان هوشمند
امن پایش
AmnPaayesh
هوبان
سامانه‌ی
اتوماسیون
پارکینگ
فرجا

فصلنامه امنیت الکترونیک

صاحب امتیاز و مدیرمسئول:
محمد قلم‌چی

سردبیر:
معصومه عباسیان

هیئت تحریریه (به‌ترتیب حروف الفبا):
سیده مژگان سیدنقوی
محمد قلم‌چی
مصطفا کردی

ویراستار:
معصومه عباسیان

صفحه‌آرایی و طراحی:
معصومه عباسیان

نشانی دبیرخانه: تهران- اقدسیه- بلوار ارتش- اراج- شانزده‌متری ولیعصر- نبش خیابان پروین- پلاک ۲- واحد ٤
تلفن: ۰۲۱-۲۲۹٦۷۷٦۳
نمابر: ۰۲۱-۲۲۹٦۷۷٦۹
نشانی اینترنتی: www.electronicsecurity.ir
پست الکترونیک: info@electronicsecurity.ir

فهرست

سرمقاله

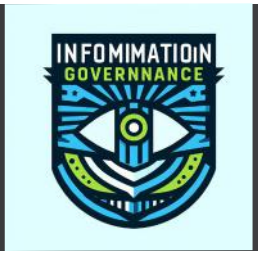
نویسنده:
محمد قلم‌چی

ارائهٔ سرویس‌های ابری سال‌هاست در کشورهای پیشرفته وارد قلمرو امنیت الکترونیکی یا به بیان دیگر حفاظت فیزیکی شده است. هم‌اکنون به‌سختی می‌توان در امریکا تجهیزات دوربین مداربسته را مستقلاً خریداری کرد، زیرا بیش از ۹۰٪ مشتریان در حال استفاده از سرویس‌های ابری جامع هستند. بازار فروش تجهیزات امنیت الکترونیکی، از دوربین مداربسته گرفته تا دزدگیر و اعلام سرقت، جایشان را به امانت تجهیزات و ارائهٔ پردازش ابری و تأمین بستر توسط اپراتورها داده‌اند.

اطمینان از کارکرد صحیح، کاهش هزینهٔ واقعی طول عمر، اطمینان از دردسترس‌بودن داده‌ها و سهولت نظارت از راه دور از مزایای اصلی خدمات جامع امنیت الکترونیک از جمله خدمت جامع نظارت تصویری (iVSaaS) است، اما مقاومت مشتریان و سازمان‌ها در تغییر فناوری، تمایل کارفرمایان به نگهداری اطلاعات نزد خود، عدم شناخت دقیق مشتری و دشواری محاسبهٔ هزینه‌های واقعیِ راه‌بردهای سنتی و عدم ارائهٔ بستر مناسب در بعضی مناطق نیز از چالش‌های کندی توسعهٔ سرویس‌های ابری امنیت الکترونیکی محسوب می‌شود.

حاکمیت اطلاعات: تعاریف و مفاهیم

اطلاعات و بزرگی حجم آن سوخت تحول دیجیتالی است که در همهٔ صنایع در حال رخ دادن است. در همان حالی که سازمان‌ها محصولات، کانال‌ها و عملیات جدیدی را توسعه می‌دهند، برای تصمیم‌گیری‌های راهبردی به اطلاعات گسترده‌تری نیاز دارند.



۲۶

پایداری در ضبط تصاویر سامانهٔ نظارت تصویری

یکی از ویژگی‌های مهم و ضروری سامانه‌های نظارت تصویری، امکان دسترسی همیشگی کاربر به تصاویر ضبط‌شدهٔ باکیفیت است.

۳۰

نشست با یاسر باقری

مدیرکل بررسی‌های اقتصادی و توسعهٔ کسب‌وکار شرکت مخابرات ایران

۳۷

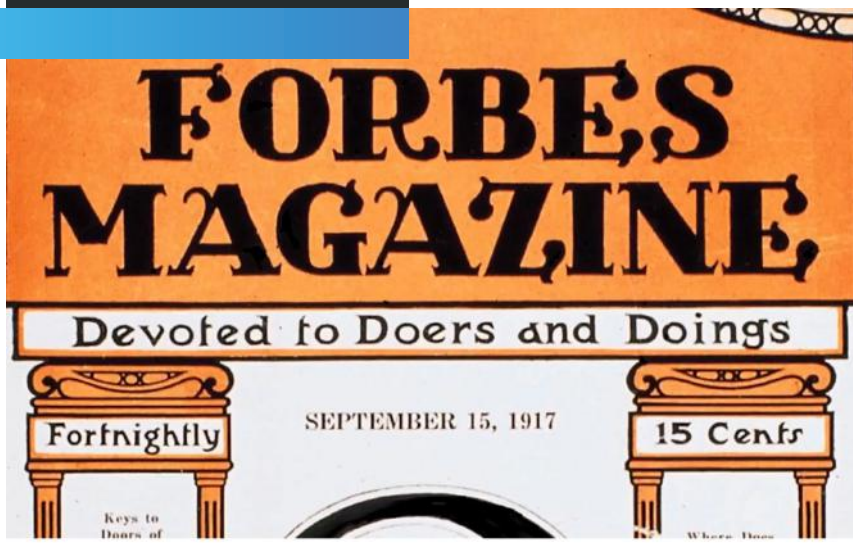
دانستنی‌های فناوری

مترجم:
مصطفا کردی

۱۴ روایت نادیده‌گرفته‌شده از فناوری که باید بدانید

هر روز هزاران رویداد خبری دربارهٔ فناوری‌های نوین و صنعت فناوری توسط رسانه‌های خبری مختلف در سراسر جهان منتشر می‌شود. حجم اطلاعات چنان عظیم است که حتی کسانی که غرق در دنیای فناوری هستند هم قادر به تعقیب اخبار تمامی این رویدادها نیستند. در حالی که هر سال بخش کوچکی از رویدادهای مرتبط با فناوری به آگاهی جهانیان می‌رسد، بخش بزرگی از آنها از دید مخاطبان پنهان می‌ماند، گرچه ممکن است برخی از آنها به‌شدت بر نحوهٔ زندگی و کار ما تأثیر بگذارند.

برخی از رویدادهای جذاب اخیر فناوری، از تغییر در استانداردهای حریم خصوصی و امنیت گرفته تا پیشرفت‌های جدید در حوزهٔ انرژی، حتی دستاوردهای بی‌سابقه در هوش مصنوعی ممکن است مورد توجه رهبران صنعت و عموم مردم قرار نگرفته باشند. آنچه در ادامه می‌آید موارد برگزیدهٔ رویدادهای فناوری از نگاه اعضای شورای فناوری در فوربس است. تلاش کرده‌ایم گزارشی ملموس از دلایل این گروه برای انتخاب این فناورهای ارائه کنیم.



فناوری‌هایی که برای افزایش محرمانگی حریم‌های مشترک ضروری هستند

جف وایت[1] بنیان‌گذار و مدیرعامل شرکت گریوی آنالیتیکز[2] که خدمات حرفه‌ای تحلیل مکان را به سازمان‌ها ارائه می‌دهد عقیده دارد که برای رسیدن به استانداردهای لازم برای حفظ محرمانگی داده‌های مشتریان لازم است فناوری‌های افزایش امنیت داده در حوزهٔ مکان‌یابی که توسط شرکت‌های خدمت‌رسان به‌کار گرفته می‌شوند، عمومیت یابند. دسترسی عام به این فناوری‌ها برای هر سازمانی که از داده‌های مشتریان استفاده می‌کند راهی برای مدیریت مطمئن این داده‌ها ارائه می‌دهد.

تغییر سیاست‌های ردیابی کاربران

بسیاری از کسب‌وکارها در سال‌های اخیر پی بردند که اثرگذاری تبلیغات آنها در

1- Jeff White
2- Gravy Analytics

این تصویر و بیشتر تصاویر این شماره با افزونهٔ تولید تصویر مایکروسافت بینگ تولید شده است. این تصویر در ارتباط با OpenAI تولید شده است.

فیس‌بوک بسیار کمتر از گذشته بوده، در حالی که هزینهٔ بیشتری برای این کار صرف کرده‌اند. تاد لوفبورو[3] مدیرعامل آژانس بازاریابی دیجیتال وایرال گینز[4] می‌گوید: «اپل تغییراتی در نحوهٔ ردیابی کاربران آیفون توسط بازاریابان ایجاد کرده است.» از این گذشته، مرورگرها نیز به حفظ بیشتر حریم خصوصی کاربران گرایش دارند. این جهت‌گیری شیوهٔ مؤثر ارتباط کسب‌وکارهای بزرگ و کوچک با مشتریان احتمالی را تغییر خواهد داد.

3- Tod Loofbourrow
4- Viral Gains

عدم استقبال از تحول دیجیتال در میان کارکنان جوان

کارکنان جوان‌تر، خصوصاً آنهایی که در مواجهه با قرنطینهٔ همه‌گیری کرونا ۲۰۱۹، فضای ناپایدار اجتماعی و اقتصادی و برآوردن مهارت‌های مختلف مدنظر کارفرما و زمان کاری غیرمعمول آسیب‌پذیر بوده‌اند، تحول دیجیتال در سازمان‌ها را به تأخیر می‌اندازند. ریکاردو مادان[5] قائم‌مقام شرکت تِک‌سیستمز[6] ادعا می‌کند که این احتمال وجود دارد که صاحب‌منصبان باسابقه در حوزهٔ فناوری این عوامل را که به‌ضرر ارتباطات تیم‌محور و مهارت‌های حل مسئله در هم تنیده شده‌اند، نادیده گرفته باشند.

5- Ricardo Madan
6- TEKsystems

بازگشت غول‌های فناوری به کارِ درمحل

تمایل به دورکاری روبه‌رشد است. با این حال، در شرایطی که بسیاری از شرکت‌ها هنوز در حال گذار و یا سازگاری با مدل‌های دورکاری هستند، غول‌های فناوری با وجود تحویل بی‌نقص و

باکیفیت کارها از راه دور، کارمندان خود را به دفاتر فراخوانده‌اند. سرخیو ماتی[7]، بنیان‌گذار شرکت ایندکس، می‌گوید: «ظهور مدل‌های هیبریدی به این معناست که تشکیل تیم‌های دورکار در سراسر جهان شتاب بیشتری گرفته و شرکت‌ها باید با واقعیت جدید سازگار شوند و پیش از آنکه به کار در محل بازگردند سیاست دورکاری را بپذیرند.»

پیشرفت‌های جدید در ممریستورها[8]

مدت‌ها بود که شتاب توسعهٔ ممریستورها، گونه‌ای از مدارهای الکتریکی نسل جدید، کاهش یافته بود، اما مجدداً این نوع از مدارها با جدیت در حال توسعه هستند. این مدارها ابزارهای یکپارچهٔ کارآمدی هستند که اطلاعات را به خاطر می‌سپارند و قابلیت یادگیری از رویدادهای گذشته در آنها تعبیه شده است. آرتور میلر[9]، مدیر فنی شرکت اکوییپیفای[10]، معتقد است ممریستورها می‌توانند روش‌های جدیدی برای محاسبات در مقیاس نانو، با قدرت محاسباتی سریع‌تر و متراکم‌تر تولید کنند، اما بسیار کمتر از حد انتظار مورد اقبال قرار گرفته‌اند.

راکتورهای ماژولار کوچک[11] (SMRs)

در جهان فناوری امروزی، راکتورهای ماژولار کوچک مولد انرژی هسته‌ای، بسیار کم موردتوجه قرار گرفته‌اند. رولاند پولزین[12] از شرکت وینگ اسیستنت[13] می‌گوید: «اگر بخواهیم گازهای گلخانه‌ای را کاهش دهیم و در همان حال نیز تقاضای فزاینده برای انرژی برق را برآورده کنیم، SMRها یک فناوری کلیدی برای پرکردن شکاف بین سوخت‌های فسیلی و انرژی‌های تجدیدپذیر خواهند بود. این فناوری‌ها، بسیار مقرون‌به‌صرفه هستند و قابلیت نصب در محل دارند و به‌کارگیری آنها در مناطق نامناسب برای استقرار نیروگاه‌های هسته‌ای موجه است.

جنبش رشد مسئولانه در میان تیم‌های نرم‌افزاری

در حالی که تحول اقتصادی در دستورکار تمامی شرکت‌ها و مؤسسه‌ها قرار دارد، تغییر طرز تفکر تیم‌های نرم‌افزاری از «رشد به هر قیمتی» به «رشد مسئولانه» بر تک‌تک تیم‌ها تأثیر خواهد گذاشت. مهم‌ترین نکته همین ادعای مایا ماندل[14] مدیر محصول شرکت هلیوس[15] است: «نگاه به درون و جست‌وجوی راه‌های هوشمندانه برای ارزش‌آفرینی به شیوه‌ای پایدار» رویهٔ روبه‌رشد دیگر بهبود تجربهٔ توسعه‌دهندگان نرم‌افزار به‌منظور افزایش کارآمدی است که به‌نوبهٔ خود باعث افزایش آگاهی نیز می‌شود.

قدرت جمع‌سپاری[16]

در سال‌های اخیر، شاهد چندین مورد از کارآمدی اجتماعات و جمع‌سپاری در تأمین و تولید محصولات و خدمات بوده‌ایم. مواردی چون بالارفتن ارزش سهام گیم‌استاپ[17] ناشی از پامپ[18] آن

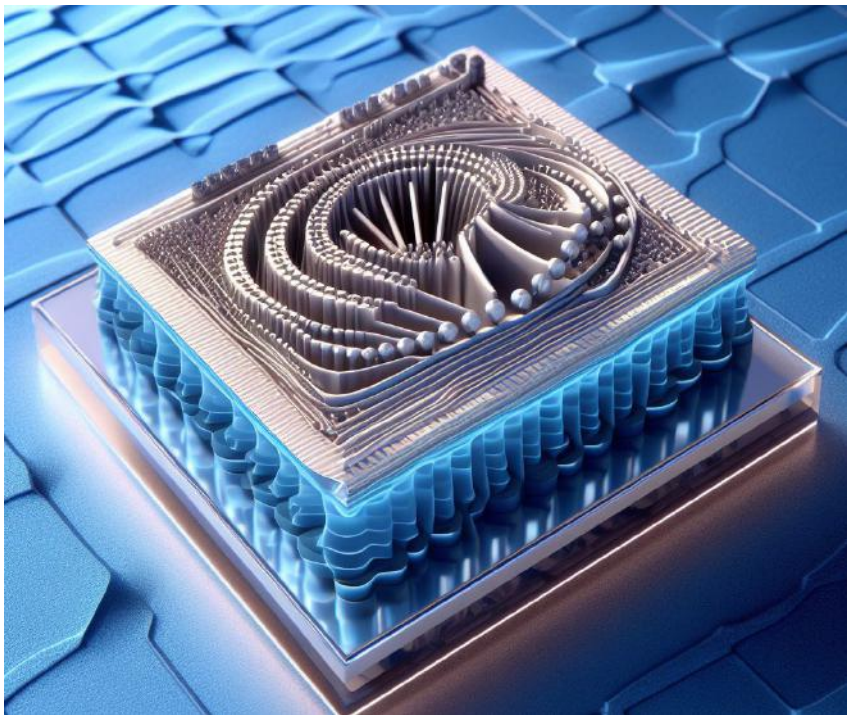
7- Sergiu Matei
8- Memristors
9- Arthur Miller
10- Equipifi
11- Small Modular Reactors
12- Roland Polzin
13- Wing Assistant

14- Maya Mandel
15- Helios

۱۶- Crowdsourcing؛ در واقع نوعی برون‌سپاری پروژه، توسعهٔ محصول یا خدمت از طریق جلب مشارکت عمومی، به‌ویژه با مراجعه به اجتماعات آنلاین، است.

17- GameStop

۱۸- Pump؛ نوسان شدید و صعودی و مشکوک رمزارز که از طریق سرمایه‌گذاری یک سرمایه‌گذار بزرگ و تبلیغاتش اتفاق می‌افتد.



توسط جامعهٔ ردیت[19]، یا سر برآوردن و رشد رمزارزهای مم[20]، که صرفاً توسط جوامع هدایت می‌شوند، یا استفادهٔ نایک و آدیداس از جوامع برای هدایت مدل‌های درآمدی مبتنی بر توکن غیرقابل‌تعویض[21] و پلتفرم‌های بازی‌های ویروسی مانند روبلاکس[22] از این دست جمع‌سپاری‌ها هستند. با وجود این، نیتین کومار[23] مدیرعامل شرکت زی‌بلاکز[24] معتقد است افراد و شرکت‌ها هنوز نتوانسته‌اند از پتانسیل مدل کسب‌وکار جامعه‌محور به‌طور کامل استفاده کنند.دنیای موجود

19- Reddit
20- Meme crypto coins
21- Nonfungible token revenue (NFT)
22- Roblox
23- Nitin Kumar
24- Zblocks

طراحی اساسا مورد استفاده قرار گیرد. لورم ایپسوم متن ساختگی با تولید سادگی نامفهوم از صنعت چاپ و با استفاده از طراحان گرافیک است. چاپگرها و متون بلکه روزنامه و مجله در ستون و سطرآنچنان که لازم است و برای شرایط فعلی تکنولوژی مورد نیاز و کاربردهای متنوع با هدف بهبود ابزارهای کاربردی می باشد.

گرایش به داده‌های طرف اول[25]

به گفتهٔ الکساندر روبیکت[26] بنیان‌گذار و

۲۵- First-Party Data؛ در دنیای کسب‌وکار داده‌ها به چهار دسته تقسیم می‌شوند: ۱. داده‌های طرف صفر که به‌صورت خودکار در اختیار شرکت‌ها قرار داده می‌شوند؛ ۲. داده‌های طرف اول که از طریق فرم‌های ثبت‌نام و مستقیماً توسط کاربران به شرکت‌ها سپرده می‌شوند؛ ۳. داده‌های طرف دوم که از طریق مشارکت در بازاریابی و سایر منابع غیررقابتی به دست می‌آیند؛ ۴. داده‌های طرف سوم یا شخص ثالث که از طریق یک جمع‌کننده مانند کارگزاری‌ها، در دسترس شرکت‌ها قرار می‌گیرند.

26- Alexander Robicquet

مدیرعامل شرکت کراسینگ ماینِدز[27] علاقهٔ سرسام‌آور به داده‌های طرف اول یک رویداد بسیار مهم و سزاوار بررسی بیشتر است. به اعتقاد او در تمامی صنایع، از خرده‌فروشی گرفته تا هنر و غیره، مدیران پی برده‌اند که استراتژی‌های هدف‌گیری نفوذی، مانند کوکی‌های شخص ثالث، شیوه‌هایی ناپایدار هستند. آنها به این مهم پی برده‌اند که داده‌های طرف اول، بهترین جایگزین برای اطمینان از شخصی‌سازی دقیق و معنادار تجربه‌های کاربر است، بدون اینکه مخاطره‌ای برای اطلاعات شناسایی شخصی مصرف‌کنندگان ایجاد کند.

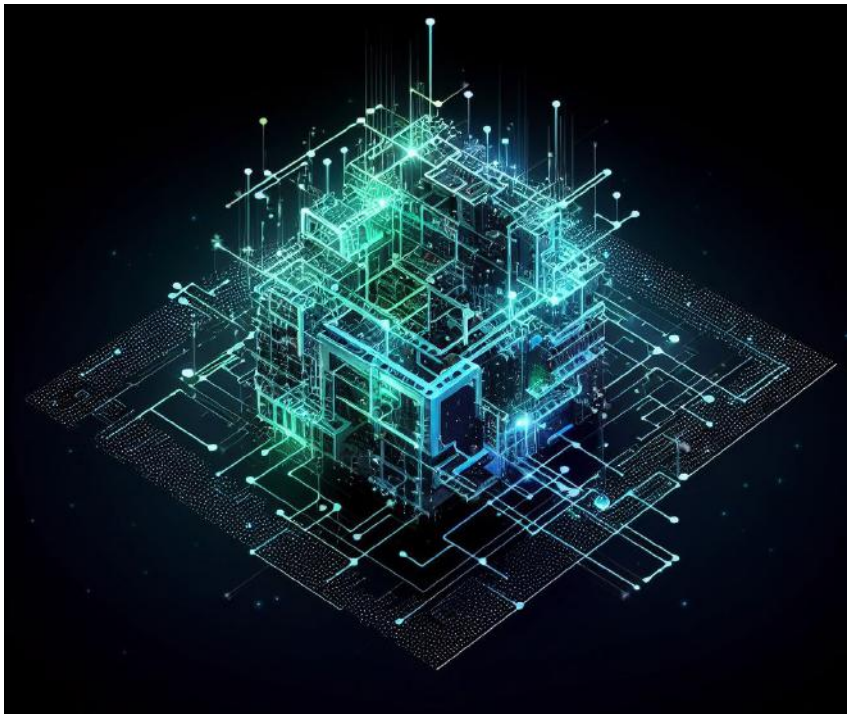
توسعهٔ فناوری جدید در حوزهٔ سلامت

از نظر نیکلاس دومنیش[28] مدیرعامل شرکت ای‌ای‌اِس هلث[29] در حالی که پس از همه‌گیری کرونا، همه بر تورم ناشی از آن متمرکز شدند، صنعت سلامت بی‌سروصدا در تمام جوانب در حال تکامل بوده است. فراتر از آن، دست‌اندرکاران صنعت سلامت در حال پیاده‌سازی فناوری‌های سلامت دیجیتال هستند که نوآوری در پذیرش بیمار، تصمیم‌گیری‌های داده‌محور و پزشکی با مدل عرضهٔ مستقیم به مشتری[30] را ممکن می‌سازد. این فناوری به‌زودی تجربه‌های همهٔ ما را در حوزهٔ بهداشت و سلامت تغییر خواهد داد.

محاسبات کوانتومی

از نظر شان توسی[31]، بنیان‌گذار و مدیرعامل شرکت گلوتری‌دی[32]، محاسبات کوانتومی این قابلیت را دارد که روش ما در حل مسئله را متحول کند و می‌تواند تأثیر قابل‌توجهی در زمینه‌هایی مانند یادگیری ماشین و هوش مصنوعی داشته باشد.

27- Crossing Minds
28- Nicholas Domnisch
29- EES Health
30- Direct to Customer (DTC)
31- Sean Toussi
32- Glo3D



هرچند هنوز تحقیقات زیادی باید در این حوزه انجام شود اما محاسبات کوانتومی، نوعی فناوری است که افراد بیشتری باید بر آن متمرکز شوند.

فشار بیش از اندازه بر سرویس‌دهندگان فناوری ابری

حسین شرف[۳۳]، مدیرعامل شرکت کلاودفورس[۳۴]، مدعی است ارائه‌دهندگان بزرگ فناوری ابری با چنان تقاضای زیادی مواجه هستند که گاهی به این خاطر در تحویل به‌موقع مراکز داده دچار مشکل می‌شوند. ازاین‌رو، او عقیده دارد که شرکت‌ها باید قبل از آغاز فرایند انتقال به فضای ابری یا پیاده‌سازی سرویس‌های جدید، برنامه‌ریزی بهتری داشته باشند و اطمینان حاصل نمایند که پلتفرم ابری انتخابی آنها منابع در دسترس و تخصیص‌یافتهٔ کافی داشته باشد.

ضرورت ارائهٔ راهکارهای بدون گذرواژه

مارک شلزینگر[۳۵] از شرکت راهکارهای مالی براودریج[۳۶] می‌گوید: «به نظر من، یکی از رویدادهای کلیدی فناوری در سال‌های اخیر که دیده نشده، اهمیت و ضرورت پیاده‌سازی راهکارهای بدون گذرواژه در پلتفرم‌ها و محصولات حساس و حیاتی است.» این روش، یکی از حیاتی‌ترین راه‌حل‌ها در بخش امنیت اطلاعات به‌شمار می‌رود و مزایای زیادی در بهبود قابل‌توجه ضعیف‌ترین اجزای محصول دارد.

استفاده از هوش مصنوعی در هنر و تولید محتوا

در سال ۲۰۲۲، یک هنرمند از ابزار هوش مصنوعی برای ایجاد یک اثر هنری دیجیتال استفاده نمود و برندهٔ مسابقهٔ هنرهای زیبا در نمایشگاه ایالت کلرادو شد. مت برسث[۳۷]، بنیان‌گذار و معاون فناوری اطلاعات شرکت اِن‌ال‌پی لاجیکس[۳۸]، با این خبر صحبتش را آغاز می‌کند و در ادامه می‌گوید: «فکر می‌کنم تأثیری که امروزه هوش مصنوعی بر فرایندهای خلاق خواهد گذاشت دست‌کم گرفته شده است. تولید محتوای مبتنی بر هوش مصنوعی، یک تحول و دگرگونی عظیم خواهد بود.» مایکروسافت نیز پیش از این اعلام کرده بود که افزونهٔ دال-ای ۲[۳۹] را در مایکروسافت دیزاینر[۴۰]، در رقابت با کانوا[۴۱]، برای کمک به طراحان ایجاد کرده است و این تازه شروع ماجراست.

33- Husein Sharaf
34- Cloudforce
35- Mark Schlesinger
36- Broadridge
37- Matt Berseth
38- NLP Logix
39- DALL-E 2
40- Microsoft Designer
41- Canva

تازه‌های ۲۰۲۳ در نظارت تصویری

با ورود به سال ۲۰۲۳، صنعت نظارت تصویری به سبکی جدید در حال تغییر است. راه‌حل‌های خلاقانه‌ی هوش مصنوعی (AI) و سامانه‌های یکپارچه، شیوه‌ی استفاده‌ی کسب‌وکارها از سامانه‌های نظارت تصویری را متحول می‌کنند.

مترجم:
مصطفا کردی

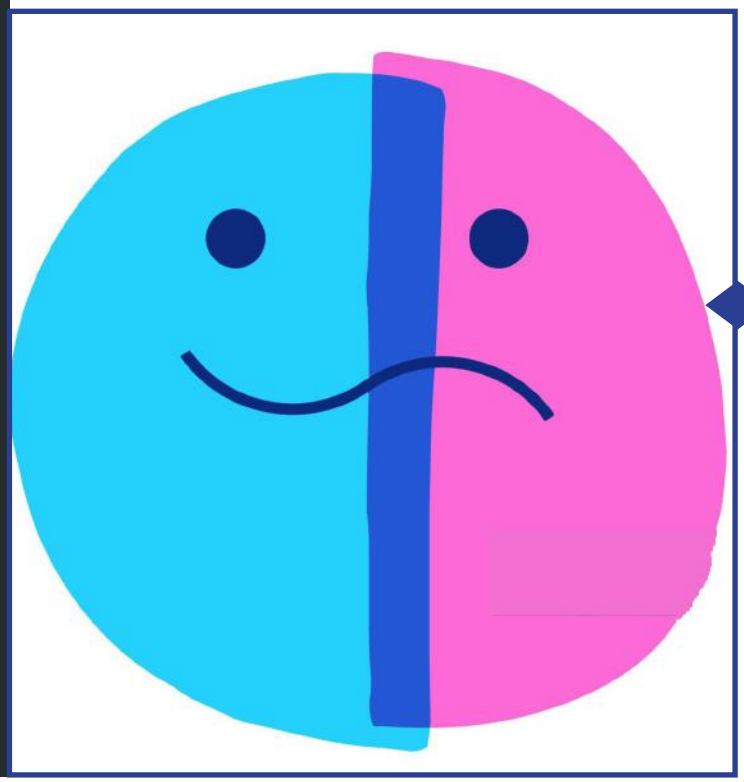
در همین حال، کسب‌وکارها در حال برداشتن گام‌هایی برای مواجهه با آیندهٔ اقتصادی نامطمئن هستند و از درس‌های آموخته‌شده در طول همه‌گیری برای اتخاذ تصمیم‌های تجاری عاقلانه استفاده می‌کنند.

[در این گزارش] کارشناسان ایگل‌آی نتورکز[1] پیش‌بینی کرده‌اند که صنعت نظارت تصویری در سال ۲۰۲۳ به کدام سو می‌رود، همچنین مواردی که بر صنعت نظارت تصویری در سال ۲۰۲۳ تأثیر می‌گذارد، توضیح داده شده است و نکاتی آمده است که رهبران کسب‌وکار باید به‌کار ببندند تا از این تغییرات برای بهبود عملکرد خود استفاده کنند.

1- Eagle Eye Networks

روند ۱: کسب‌وکارها درصدد راه‌اندازی پلتفرم‌های نظارت تصویری مجهز به هوش مصنوعی هستند

کسب‌وکارهای موفق در حال آماده‌شدن برای آینده هستند و مایل‌اند از سامانه‌های نظارت تصویریِ مجهز به هوش مصنوعی، که قابلیت اجرای تحلیل‌های [تصویری] پیشرفته را دارند، استفاده کنند. تغییرات پردامنه در چند سال گذشته در شیوهٔ تجارت در جهان، شرکت‌ها را مجبور کرد که فناوری‌ها را به روش‌های جدیدی به‌کار بگیرند. سامانه‌های نظارت تصویری که زمانی فقط به‌منظور امنیت استفاده می‌شدند، اکنون ابزاری برای کمک به بهینه‌سازی عملیات تجاری



دغدغه‌های مشتریان:

٪۵۰ نگران بهبود امنیت و عملیات پارکینگ هستند.

٪۲۷ نگران امنیت پارکینگ خود هستند.

٪۲۳ خواسته‌ای ندارند.

هستند. گرایش کسب‌وکارها به استفاده از سامانه‌های نظارت تصویری مجهز به هوش مصنوعی برای کسب اطلاعات مفید از داده‌های جمع‌آوری شده است.

بر پایهٔ نتایج یک نظرسنجی دربارهٔ کسب‌وکار هوش مصنوعی در سال ۲۰۲۲ توسط پرایس واترهاوس کوپرز[2]، بیش از ۵۰ درصد از کسب‌وکارها به نوعی از هوش مصنوعی استفاده می‌کنند و بیش از ۲۵ درصد از آنها گزارش داده‌اند که به‌طور گسترده از هوش مصنوعی در شرکت خود استفاده می‌کنند. این نظرسنجی نشان می‌دهد که کسب‌وکارهایی که هنوز از هوش مصنوعی استفاده نمی‌کنند می‌دانند که فناوری‌های جدید سامانه‌ها و فرایندهای آنها را در آینده خودکار می‌کنند و از حالا برای زیرساخت‌هایشان برنامه‌ریزی می‌کنند.

سامانه‌های نظارت تصویری مجهز به هوش مصنوعی، به کسب‌وکارها کمک می‌کنند تا توانایی خود را برای تجزیه‌وتحلیل داده‌ها افزایش دهند. کاربردهای پیشرفتهٔ [این فناوری] شامل سامانه‌هایی است که می‌توانند به‌طور خودکار هشدارهای تهدیدهای امنیتی را شناسایی و ارسال کنند و داده‌های مربوطه را گردآوری نمایند تا اطلاعات مفیدی مانند اوج رفت‌وآمد افراد یا زمان انتظار مشتری را استخراج کنند.

کسب‌وکارهایی که با رایانش ابری آشنا هستند می‌دانند که [فناوری] ابری بهترین گزینه آینده‌نگرانه برای [برخورداری از] ویژگی‌های پیشرفته و فراگیر در سامانه است. با استفاده از [فناوری] ابری، کسب‌وکارها از سرمایه‌گذاری، نگهداری و ارتقای سخت‌افزار و نرم‌افزار بی‌نیاز می‌شوند. بدین ترتیب هزینه‌های فناوری اطلاعات به‌طور چشمگیری کاهش می‌یابد. [فناوری] ابری مقیاس‌پذیری، انعطاف‌پذیری و قابلیت اطمینان را نیز برای کسب‌وکارها به‌ارمغان می‌آورد و به آنها امکان می‌دهد ویژگی‌های مبتنی بر هوش مصنوعی را [به سامانهٔ خود] اضافه کنند. به‌طور خلاصه، رایانش ابری شایسته‌ترین میزبان برای هوش مصنوعی پیشرفته است و کسب‌وکارهایی که امروز آن را پذیرفته‌اند، فردا در موقعیت خوبی برای رقابت در بازار جهانی خواهند بود. کسب‌وکارهای موفق، بازگشت سرمایهٔ استفاده از سامانه‌های نظارت تصویری مجهز به هوش مصنوعی را درک می‌کنند و سامانه‌ای می‌خواهند که با پیشرفت‌های هوش مصنوعی و تحلیل تصاویر هماهنگ باشد.

روند ۲: کسب‌وکارها راهکارهایی می‌خواهند که هزینه‌های عملیاتی را کاهش دهد

هزینهٔ انجام کسب‌وکار همچنان در حال افزایش است و بسیاری از شرکت‌ها به‌دلیل نحیف‌شدن حاشیهٔ سود، در امور مالی خود سخت‌گیرانه می‌نگرند. تورم به بالاترین حد خود در ۴۰ سال اخیر رسیده است، صنایع همچنان با مشکلات زنجیرهٔ جهانی تأمین، کمبود مداوم تراشه‌های نیمه‌هادی و کمبود نیروی کار دست‌وپنجه نرم می‌کنند. شرکت‌ها برای مواجهه با یک آیندهٔ اقتصادی نامشخص گام برمی‌دارند و گزینه‌هایی برای کاهش هزینه‌های عملیاتی از جمله برای سامانه‌های نظارت تصویری خود می‌خواهند.

هزینه‌های فناوری عملیاتی که بسیاری از آنها غیرمشهودند می‌توانند باعث افزایش قابل‌توجه هزینهٔ مالکیت فناوری شوند. با

> کسب‌وکارها می‌دانند که با سرمایه‌گذاری در راهکارهای هوش مصنوعی مبتنی بر [فناوری] ابری، می‌توانند امنیت و فرایند عملیاتی خود را بهبود بخشند و در درازمدت هزینه‌ها را کاهش دهند.

2- PricewaterhouseCoopers

افزایش سه‌برابری دوربین‌های امنیتی IP با وضوح بالا در ۵ سال گذشته

این حال، فناوری مبتنی بر ابر [امکان] صرفه‌جویی قابل‌ملاحظه‌ای را در اختیار کسب‌وکارها می‌گذارد. انتقال زیرساخت محاسباتی و ذخیره‌سازی ویدئو به فضای ابری منجر به کاهش هزینهٔ کلی مالکیت در مقایسه با یک سامانهٔ معمولی مستقر در محل می‌شود. افزایش طول عمر [تجهیزات] عموماً بین ۲۰ تا ۵۰ درصد در مقایسه با هزینهٔ میزبانی برنامه‌های کاربردی VMS (سامانهٔ مدیریت ویدئو) در مرکزدادهٔ شرکت متفاوت است.

برخی از ارائه‌دهندگان VSaaS (نظارت تصویری به‌عنوان خدمت) اکنون در ازای اشتراک‌های چندساله تخفیف و حمایت در برابر افزایش قیمت‌های ناشی از تورم در آینده را پیشنهاد می‌دهند. [به این ترتیب] مشتریان تشویق می‌شوند تا برای اشتراک سالانه یا چندساله ثبت‌نام کنند تا از قیمت‌های امروزی که در طول مدت اشتراک افزایش نمی‌یابد استفاده کنند.

در حالی که برخی از مشتریان به انعطاف‌پذیری صورت‌حساب ماهانه متکی هستند، بیشتر کسب وکارها ترجیح می‌دهند برای خدماتی که حق اشتراک دارند و قبلاً بودجه‌بندی شده‌اند سالی یک بار پرداخت انجام دهند. قراردادهای خدمات با تخفیف و صورت‌حساب انعطاف‌پذیر تا زمانی که اقتصاد تثبیت نشود، همچنان گریبان‌گیر کسب‌وکارها خواهند بود.

و نکتهٔ آخر اینکه کسب‌وکارها به‌دلیل مقرون‌به‌صرفه‌تر شدن دوربین‌هایی با وضوح بالاتر خریداری می‌کنند. طبق گزارش سال ۲۰۲۳ ایگل‌آی فروش دوربین نظارت تصویری با وضوح بالا طی پنج سال گذشته افزایش سه برابری داشته است. با افزایش وضوح توانایی پیاده‌سازی راهکارهای تحلیل ویدئویی نیز افزایش می‌یابد و در نهایت سامانه‌ها را اثربخش‌تر می‌کند.

از هر ٤ مشتری احتمالی، ۳ نفر خواستار راهکارهایی برای پارکینگ هستند

روند ۳: پارکینگ در سراسر جهان خودکار می‌شود

بازار سامانهٔ پارکینگ خودکار رشد فوق‌العاده‌ای داشته است. کسب‌وکارهایی که انواع پارکینگ را، از ساختمان‌های چندخانواری و پارک‌های تجاری گرفته تا ساختمان‌های تجاری و مجتمع‌های پزشکی، مدیریت می‌کنند به‌دنبال راهکار ساده‌ای هستند.

بر اساس گزارش سال ۲۰۲۲ از ایمرجن ریسرچ[3] انتظار می‌رود بازار سامانهٔ پارک خودکار تا سال ۲۰۳۰ با نرخ مرکب سالانه (CAGR) ۱۵٫۱ درصدی رشد کند. بر همین پایه پیش‌بینی می‌شود، ارزش بازار در این مدت رشد ۳ میلیارد دلاری را تجربه کند. افزایش مداوم [تعداد] وسایل نقلیه در معابر به‌علاوهٔ کمبود زمین و راحتی مصرف‌کننده به رشد این بازار کمک می‌کند.

در نظرسنجی ایگل آی از تجمیع‌کنندگان سامانه‌های امنیتی، ۵۰ درصد از پاسخ‌دهندگان گفتند که مشتریان بالقوهٔ آنها از بهبود امنیت و عملکرد پارکینگ‌ها سؤال کرده‌اند. در همین حال، ۲۷ درصد از مشتریان بالقوه در مورد امنیت محل پارک خود پرسش داشتند در حالی که ۲۳ درصد از مشتریان احتمالی به طور خاص راجع به پارکینگ سؤال نکردند.

روند ٤: مدارس در حال آزمایش فناوری‌های امنیتی برای افزایش ایمنی هستند

بهبود ایمنی محوطه مدرسه به ویژه در ایالات متحده همچنان در اولویت است. در نتیجه انواع فناوری‌های امنیتی در اختیار گرفته می‌شوند. مدارس در حال بررسی و استفاده از سامانه‌های امنیتی برای ایمن‌تر کردن ادامه می‌دهند. در حالی که [کارآیی] هیچ راه حل واحدی برای حل همه مشکلات ایمنی و امنیت مدارس ثابت نشده است سامانه‌های سازگار در بهترین موقعیت برای پاسخگویی به نیازهای [پایش] محوطه مدارس قرار دارند.

در تابستان ۲۰۲۲، قانونگذاران ایالات متحده

3- Emergen Research

بودجه‌ای ۱ میلیارد دلاری را برای مدارس به منظور «ایجاد محیط‌های آموزشی ایمن و سالم برای همه دانش آموزان» با ۳۰۰ میلیون دلار اضافی برای آموزش و [تمهید] تجهیزات برای بازدارندگی در برابر تهدید مدارس تصویب کردند.

آنچه مدارس می‌خواهند، راه‌حل‌هایی برای بهبود بازدارندگی، شناسایی و

نظارت تصویری همراه با کنترل دسترسی و سیستم‌های ارتباطی از رایج‌ترین اقدامات امنیتی هستند که مدارس در آن سرمایه‌گذاری می‌کنند.

واکنش در برابرحوادث است. نظارت تصویری برای بخش آموزش باید به راحتی با سایر برنامه‌های امنیتی ادغام شود تا توانایی سامانه را افزایش دهد. قابلیت ترکیب برنامه‌های کاربردی کنترل دسترسی با نظارت تصویری سامانه‌ها را در بازار بخش آموزش متمایز می‌کند.

مدیران مدرسه و تیم‌های فناوری اطلاعات به سامانه‌ای نیاز دارند که استفاده از آن آسان باشد و میزان تجهیزات و عملیات نگهداری در محل را کاهش دهد. نظارت تصویری ابری یک پلتفرم ایده‌آل را در اختیار می‌گذارد که امکان مدیریت متمرکز همه امکانات را از یک داشبورد فراهم می‌کند.

مدارس به دنبال گزینه‌های پیشرفته‌ای مانند تجزیه و تحلیل ویدئو نیز هستند که به صورت خودکار هشدارهایی را هنگام ورود افراد به محوطه‌های مختلف آموزشگاه مانند پارکینگ‌ها یا زمین‌ها ورزش در ساعات غیرفعال ارسال می‌کنند. آنها همچنین خواهان یک راه آسان برای دسترسی و به اشتراک گذاری نظارت‌تصویری با مراجع ذیربط در هنگام حوادث بحرانی هستند.

برخی از سامانه‌های نظارت تصویری به مدیران اجازه می‌دهند تا به‌صورت پیش‌تنظیم‌شده به اولین مرجع ذی‌ربط اجازه دهند تا در مواقع اضطراری بتواند به ویدئوی زنده دسترسی داشته باشد.

به طور کلی، سامانه مدارس در بخش سامانه‌های امنیتی ارتقا یافته بازار قرار می‌گیرند اما این سامانه‌ها باید ویژگی‌های پیشرفته‌ای را فراتر از آنچه که یک سامانه نظارت سنتی ارائه می‌دهد در اختیار بگذارند تا نسبت به فناوری‌های رقیب در اولویت قرار داده شوند.

سامانه‌های امنیتی کنونی باید ویژگی‌های پیشرفته‌تری از سامانه‌های نظارتی سنتی ارائه دهند تا بتوانند با سایر فناوری‌ها رقابت کنند

روند ۵: پشتیبانی آسان و مستمر مشتری باعث

صرفه‌جویی در زمان و نیروی انسانی می‌شود

بیشتر کسب‌وکارها می‌دانند خدمات آموزشی و پشتیبانی مشتری به این خاطر ارزشمند هستند که تأثیری انکارنشدنی بر تصمیم مشتری راجع به خرید محصول می‌گذارند. مشتریان انتظار دارند خدمات به‌صورت ۲۴ساعته و به شکل فوری و آسان به ایشان عرضه شود. می‌توان گفت نحوهٔ ارائهٔ خدمات، در حال تبدیل‌شدن به وجه متمایزکنندهٔ راهکارهای امنیتی است.

در حال حاضر از هر ۱۰ کسب‌وکار، بیش از ۹ تای آنها به‌نوعی از فناوری ابری، از جمله در [خدماتی چون] ایمیل، تلفن، پشتیبان‌گیری، برنامه‌های [کاربردی] و به‌طور فزاینده‌ای در حوزهٔ نظارت تصویری استفاده می‌کنند. حالا که کسب‌وکارها به‌سمت مدل‌های SaaS (نرم‌افزار به‌عنوان خدمت) پیش می‌روند، پشتیبانی و آموزش‌های مرتبط را به‌عنوان بخشی از سرمایه‌گذاری در نظر می‌گیرند.

از سویی رهبران حوزهٔ فناوری اطلاعات تمایل بیشتری برای به‌کارگیری [راهکارهای] SaaS دارند و از سوی دیگر تمهید ارائهٔ خدمات به مشتریان بر نیاز به استخدام کارکنان تأثیر می‌گذارد. سامانه‌های مبتنی بر فناوری ابری، پشتیبان فنی را قادر می‌سازند به سامانه دسترسی پیدا کند و از راه دور مشکل را حل کند، بدین ترتیب کسب‌وکارها نیاز ندارند نیروی متخصص استخدام کنند و می‌توانند در هزینه‌های عملیاتی صرفه‌جویی کنند.

مشتریان به‌صورت ۲۴ساعته انتظار خدمات مشتری فوری و راحت دارند.

نویسنده:
محمد قلم‌چی

این WORM یک کِرم نیست

ذخیره‌ی اسناد مهمی مانند گزارش‌ها و تراکنش‌های مالی، سوابق ارتباطات با مشتری، اسناد راهبردی و بسیاری از اطلاعات کسب‌وکارها، حالا دیگر تقریباً به‌طور کامل در قالب الکترونیکی نگهداری می‌شوند.

تصمیم‌های اساسی تجاری بیشتر مبتنی بر اطلاعات حاصل از این داده‌ها گرفته می‌شوند و ازاین‌رو باید به شیوه‌ای قابل‌اعتماد، ایمن از تخریب یا دست‌کاری، مخفیانه نگهداری شوند.

نگهداری سوابق قابل اعتماد برای یک سازمان در قالب اطلاعات نظارتی و تجاری حیاتی است و به سازمان کمک می‌کند عملکردی روان و پیش‌رونده داشته باشد و خطرهای ناشی از دست‌کاری و از دست رفتن اطلاعات را کاهش می‌دهد.

وُرم[1] یک روش ذخیره‌سازی داده است که در آن اطلاعات پس از نوشتن قابل‌تغییر نیستند. این روشِ محافظت از نوشتن، این اطمینان را ایجاد می‌کند که داده‌ها پس از نوشته‌شدن روی دستگاه ذخیره‌ساز قابل‌دست‌کاری نباشند.

در دستگاه‌های معمولیِ ذخیره‌سازی داده (غیروُرم)، تعداد دفعات تغییر داده‌ها فقط به طول عمر دستگاه محدود می‌شوند، زیرا اصلاح (تغییر داده) شامل تغییرات فیزیکی است که ممکن است باعث فرسودگی دستگاه شود. «خواندن چندباره» موضوع قابل‌توجهی نیست، زیرا در دستگاه‌های ذخیره‌سازی مدرن خواندن داده‌ها به دفعات نامحدود پس از نوشتن مجاز است[2].

وُرم امنیت اصالت فایل‌های مهم و همچنین اعتبار داده‌ها را با دست‌نخورده نگه‌داشتن آنها تضمین می‌کند. این فناوری با از بین بردن خطر حذف یا اصلاح داده‌های مهم

1- Write Once Read Many

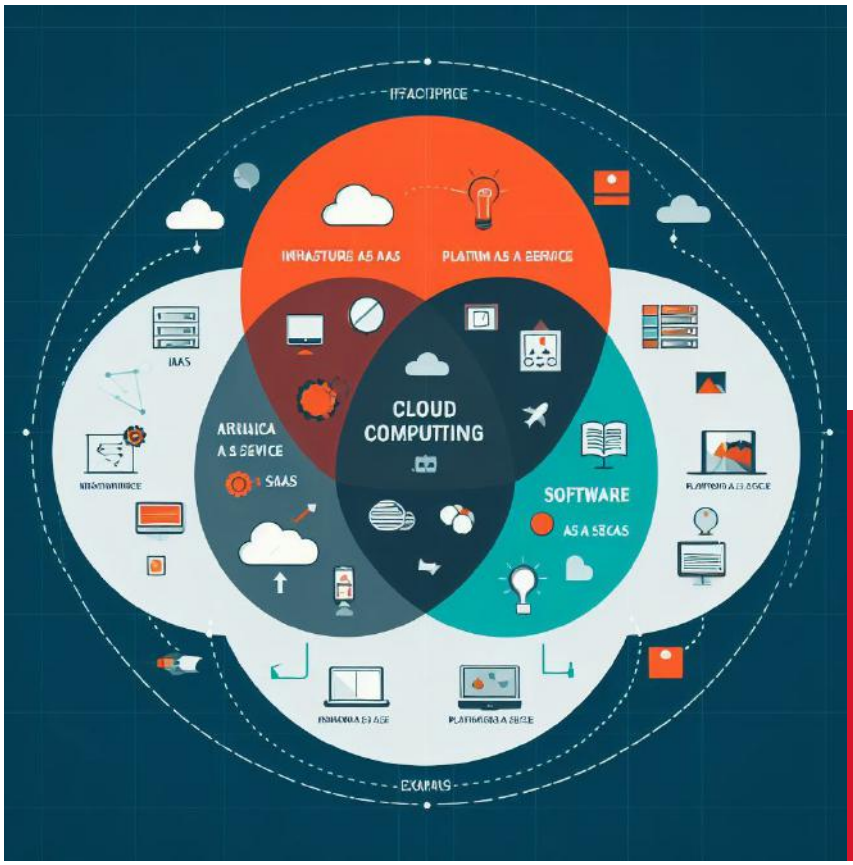
۲- البته در این مورد استثناهای تاریخی نیز وجود دارد، نظیر دیسک‌های محدود زمانی مانند Flexplay که برای اجارهٔ کوتاه‌مدت فیلم‌ها طراحی شده بودند و فناوری‌های اولیهٔ حافظهٔ غیرفرار مانند حافظهٔ هستهٔ مغناطیسی و حافظهٔ حبابی که خواندن داده‌ها در آنها موجب پاک‌شدن دادهٔ خوانده‌شده می‌شد.

بالاتریـن سـطح یکپارچگـی و امنیـت را بـرای داده‌هـا فراهـم می‌سـازد و بـه ایـن ترتیـب بـه حفـظ صحـت و ایمنـی داده‌هـای ثبت‌شـده کمـک می‌کنـد.

تاریخچهٔ فناوری وُرم

اوایـل، اسـتفاده از دیسـک فشـردهٔ نـوری در دسـتگاه‌های وُرم رایـج بـود. در ایـن دیسـک‌ها، هیـچ ناحیـه‌ای بـرای بـار دوم قابل‌ذخیـره نیسـت. بـا ایـن حـال، ایـن دیسـک‌ها غالبـاً از یـک سیسـتم فایلـی مبتنـی بـر اسـتاندارد ایـزو ۹۶۶۰ اسـتفاده می‌کننـد کـه بـه فایل‌هـای اضافـی و حتـی نسـخه‌های اصلاح‌شـدهٔ یـک فایـل بـا همـان نـام، در ناحیـه‌ای دیگـر از دیسـک اجـازهٔ ذخیـره می‌دهنـد. بـه ایـن ترتیـب بـرای کاربـر ایـن تصـور به‌وجـود می‌آیـد کـه تـا پرشـدن تمـام فضـای دیسـک، امـکان افـزودن یـا حتـی بازنویسـی اطلاعـات روی آن وجـود دارد. برخـی کارت‌هـای حافظه چندین سـازوکار حفاظتـی در برابـر نوشـتن غیرمجـاز دارنـد. رایج‌تریـن شـکل آن «کلیـد مکانیکـی محافظـت در برابـر نوشـتن» در گوشـهٔ کارت‌هـای حافظـه بـا انـدازهٔ بزرگ اسـت. ایـن کلیـد بـه کاربـر امـکان می‌دهـد تـا از کارت حافظـهٔ رایانـهٔ میزبـان به‌صـورت فقـط خواندنـی اسـتفاده کنـد. امـا اگـر رایانـهٔ میزبـان در معـرض خطـر ناشـی از آلودگـی نرم‌افـزاری باشـد، ایـن کلیـد ممکـن اسـت از داده‌هـای روی کارت محافظـت نکنـد[3].

فروشـندگان متعـددی در اوایـل دهـهٔ ۲۰۰۰ شـروع بـه سـاخت دسـتگاه‌های وُرم مغناطیسـی کردنـد. ایـن دسـتگاه‌های ذخیره‌سـازی و بایگانـی از فناوری‌هـای



جدول ۱- مقایسهٔ انواع معماری پیاده‌سازی as a Service

Traditional On-Premises IT	Colacation	Hosting	IaaS	PaaS	Sa
Data	Data	Data	Data	Data	Da
Application	Application	Application	Application	Application	Appli
Databases	Databases	Databases	Databases	Databases	Data
Operating System	Operating System	Operating System	Operating System	Operating System	Oper Sys
Vitualization	Vitualization	Vitualization	Vitualization	Vitualization	Vitual
Physical Servers	Physical Servers	Physical Server	Physical Server	Physical Server	Phy Ser
Network & Storage	Network & Storage	Network & Storag	Network & Storag	Network & Storag	Net & St
Data Center	Data Center	Data Center	Data Center	Data Center	Data

Self-Managed Provider-Managed

3- https://www.sdcard.org/downloads/pls/

مبتنی بر معماری‌هایی چون RAID[4] و فناوری‌های مغناطیسی برای ایمن‌کردن داده‌ها در برابر تغییر یا دست‌کاری غیرمجاز در سطوح سخت‌افزاری و نرم‌افزاری استفاده می‌کنند. همان‌طور که هزینهٔ ذخیره‌سازی مغناطیسی (و حالت جامد) کاهش یافته است، هزینهٔ این فناوری‌های ذخیره‌سازی آرشیوی نیز کاهش پیدا کرده است. این فناوری‌ها تقریباً همیشه مستقیماً در یک سیستم مدیریت محتوا یا اسناد ادغام می‌شوند که برنامه‌های نگهداری و کنترل دسترسی را همراه با سابقهٔ سطح اهمیت سند مدیریت می‌کنند.

فروشنده‌های متعددی از جمله EMC Centera، NetApp و KOM Networks فناوری‌های ذخیره‌سازی مغناطیسی ارائه می‌دهند. در سال ۲۰۱۳، GreenTec-USA هارد دیسک‌های وُرمی را با ظرفیت ۳ ترابایت و بیشتر توسعه داد. در این محصول حفاظت در برابر بازنویسی دیسک به‌صورت فیزیکی انجام می‌شود و نمی‌توان آن را تغییر داد یا توسط رایانه‌ای که به آن متصل‌شده لغو کرد.

با افزایش حجم داده‌های تولیدشده در سال‌های اخیر در سازمان‌ها، هزینه‌های ایجاد، نگهداری و به‌روزرسانی تجهیزات و زیرساخت‌های محلی افزایش قابل‌ملاحظه‌ای یافته است. از طرفی محبوبیت محصولات aaS[5] مانند SaaS[6]، IaaS[7] و PaaS[8] که همه بر بستر فناوری ابری شکل می‌گیرند فناوری ذخیره‌سازی را دگرگون کرده است. معماری این محصولات در جدول ۱ برای مقایسه به تصویر کشیده شده است.

تعبیهٔ وُرم در ذخیره‌سازهایِ مبتنی بر فناوری ابری از سوی شرکت‌های متعددی چون آمازون و مایکروسافت نمونه‌هایی از این دست هستند. تأمین‌کنندگان مختلف در رقابتی تنگاتنگ در حالی که تلاش می‌کنند قوانین تنظیم‌گری و تطابق را به‌دقت در راهکارهای خود رعایت کنند، می‌کوشند تا با ایجاد سیاست‌های امنیتی متنوع به جذابیت پیشنهادات خود بیفزایند. وبسایت explodingtopics.com، «معماری مبتنی بر عدم اعتماد»[9] را به‌عنوان یکی از روندهای ذخیره‌سازی امن در سال ۲۰۲۳ معرفی کرده و وُرم را یکی از اجزای پیاده‌سازی آن دانسته است.

ذخیره‌ساز وُرم چگونه کار می‌کند

به‌طور کلی دو راه برای پیاده‌سازی ذخیره‌ساز وُرم در سازمان وجود دارد. روش اول، روش سخت‌افزاری است که با استفاده از نوارهای ضبط

اطلاعات یا سایر رسانه‌هایی که داده‌ها را به‌صورت دائمی نگهداری می‌کنند و محدودکردن امکان پاک‌کردن اطلاعات به روش‌های تخریب فیزیکی دستگاه‌های ذخیره‌ساز پیاده‌سازی می‌شود.

روش دوم بهره‌گیری از خدمات ابری است. از آنجایی که بیشتر راهکارها به‌سمت سرویس‌های ابری و SaaS رفته‌اند، انتخاب یک سخت‌افزار خاص [برای ذخیره‌سازی] دشوار به نظر می‌رسد. بسیاری از ارائه‌کنندگان چنین خدماتی راهکارهایی برای پیاده‌سازی وُرم مبتنی بر نرم‌افزار ارائه کرده‌اند که هم‌زمان هم از انعطاف‌پذیری نرم‌افزار و هم از استحکام، امنیت و ماندگاری وُرم مبتنی بر سخت‌افزار برخوردارند.

صرف‌نظر از اینکه برای رسیدن به هدف موردنظر از سخت‌افزار یا نرم‌افزار استفاده شود، اصول کار در بیشتر موارد یکسان هستند. هنگامی که یک نفر داده‌هایی را به درایو وُرم اضافه می‌کند آن داده‌ها به‌صورت دائمی ذخیره می‌شوند. ایدهٔ امکان ویرایش داده‌های روی درایو وُرم تنها در مورد داده‌هایی که قبلاً ذخیره شده‌اند، اعمال می‌شود و وجود فضای کافی برای ذخیرهٔ داده روی درایو همواره امکان افزودن داده‌های جدید را فراهم می‌کند.

کاربرها می‌توانند بدون هیچ تنظیمات امنیتی یا اجازهٔ دسترسی همهٔ داده‌های روی درایو را بخوانند اما هیچ‌کدام امکان ویرایش آنچه را از قبل روی درایو بوده، ندارند. این داده برای همهٔ کسانی که به درایو دسترسی پیدا می‌کنند «فقط خواندنی» است. به این ترتیب هنگامی که مثلاً حسابرس‌ها یا کارکنان اداری نیاز دارند به سوابق و اطلاعات بایگانی‌شده مراجعه کنند، مطمئن هستند که این سوابق و اطلاعات در همان شرایطی قرار دارند که روز نخست ثبت شده‌اند و اصالت داده‌ها در این سامانهٔ ذخیره‌سازی قطعی است.

فناوری‌های ذخیره‌سازی استفاده‌شده در وُرم

رسانه‌هایی که وُرم‌ها بیشتر مبتنی بر آنها تولید می‌شوند به شرح زیر هستند:

4- Redundant Array of Independant Disks
5- as a Service
6- Software as a Service
7- Infrastructure as a Service
8- Platform as a Service
9- Zero-Trust Architecture

ذخیره‌ساز وُرم به کاربران مجاز امکان می‌دهد که به آن اطلاعاتی اضافه کنند یا اطلاعاتی از آن بخوانند، اما امکان حذف یا ویرایش اطلاعات قبلی برای آنان وجود ندارد.

- دیسک سخت
- دیسک نوری
- درایو حالت جامد[10]
- نوار مغناطیسی ذخیرهٔ داده[11]

مقایسهٔ رسانه‌های بهینه در وُرم

از آنجا که دیسک‌های سخت و درایوهای حالت جامد، در حجم گسترده، نسبت به دیسک‌های نوریِ بلو-رِی و نوار مغناطیسی، هزینهٔ تمام‌شدهٔ بالاتری دارند و همچنین خطراتی همچون ضربه برای دیسک سخت و قطع‌شدن برق برای درایو حالت جامد ممکن است باعث از بین رفتن کامل اطلاعات آنها شود، در این بخش صرفاً بلو-رِی و نوار مغناطیسی مقایسه می‌شوند.

استفاده از بلو-رِی برای ذخیره‌سازی داده‌های شرکتی، ایدهٔ نسبتاً جدیدی است، اما لزوماً روش ذخیره‌سازی مناسبی برای همهٔ مشاغل نخواهد بود. پس چرا فیس‌بوک از این فناوری به‌جای فناوری‌های معتبر دیگر استفاده می‌کند؟

گزارش شده است که فیس‌بوک در وهلهٔ اول در حال آزمایش یک کتابخانهٔ دیسک نوری بلو-رِی برای ذخیرهٔ داده‌های مطابقت[12] است. بلو-رِی از رسانه‌های قابل‌نوشتن مجدد و همچنین وُرم پشتیبانی می‌کند. داده‌های روی دیسک‌های وُرم را نمی‌توان تغییر داد، فقط می‌توان دیسک را از بین برد، بنابراین انواع رسانه‌های وُرم برای ذخیرهٔ اطلاعاتی که باید در حالت اولیهٔ خود نگهداری شوند، مانند داده‌های مطابقت و مقررات، مناسب هستند.

نقطه‌ضعف بلو-رِی این است که ظرفیت آن مجدداً قابل‌استفاده نیست، بنابراین برای هر داده‌ای که طبق مقررات لازم است حذف شود نظیر حساب‌های کاربری نامناسب است و طبق تعریف همیشه برای ذخیرهٔ داده‌های غیرفعال استفاده می‌شود. فیس‌بوک در وهلهٔ اول به‌دنبال استفاده از ظرفیت ۱ PB برای ذخیره‌سازی سرد است. داده‌ها در ذخیره‌سازی سرد قابل‌بایگانی هستند اما نیازی به دسترسی منظم ندارند، در شبکه‌های اجتماعی کپی فیلم‌ها و عکس‌های کاربر از این دسته داده‌ها هستند که به‌منظور پشتیبان‌گیری نگهداری می‌شوند. بلو-رِی به‌طور بالقوه برای این کار مناسب است اما باید دید هزینهٔ استفاده از آن چقدر می‌شود.

نمونهٔ اولیهٔ بلو-رِی شامل تقریباً ۱۰۰۰۰ دیسک نوری و یک پتابایت داده در کابینتی به‌اندازهٔ رک بود. در جدول ۲ می‌توانید به مشخصات و هزینه‌های تقریبی یک سیستم بلو-رِی و راهبرد کتابخانهٔ نوار LTO (نوعی Tape تولید کمپانی HP) نگاهی اجمالی بیندازید. هزینهٔ نوار تا ۹۵ درصد کمتر از بلو-رِی درمی‌آید و نوار تنها نیمی از فضای رک موردنیاز بلو-رِی برای همان ظرفیت ذخیره‌سازی را اشغال می‌کند.

این مقایسه بر اساس مفروضات زیر انجام شده است:

- هزینهٔ ورق فلزی، برق، فن و رباتیک موردنیاز برای یک قفسه، برای نوار و بلو-رِی تقریباً برابر در نظر گرفته شده است.
- هزینهٔ رسانه بر اساس یافته‌های اینترنت راجع به کمترین قیمت آنلاین محاسبه شده است.
- هزینهٔ درایوها شامل هزینه‌های یادشده نمی‌شود، زیرا قیمت بسته به منبع بسیار متغیر است و در تصویر کلی، هزینهٔ درایو با هزینهٔ رسانه کم می‌شود.

طبق اطلاعات جدول مقایسه، نوار اطلاعات را شش‌برابر سریع‌تر در هر درایو و سه‌برابر ارزان‌تر از بلو-رِی انتقال می‌دهد. نوار ممکن است یکی از قدیمی‌ترین اشکال فناوری باشد، اما نوآوری نوار و رشد بالای حجم داده‌ها در بازار منجر به افزایش تقاضا برای نوار در آرشیوهای طولانی‌مدت در مقیاس بزرگ شده است.

ارمغان فناوری وُرم

به‌کارگیری هر فناوری، روش یا محصول زمانی منطقی و قابل‌دفاع به‌نظر می‌آید که منافعی مشخص و ملموس برای استفاده‌کننده داشته باشد. استفاده از فناوری وُرم نیز از این قاعده مستثنا نیست. در ادامه برخی از دستاوردهای به‌کارگیریِ این فناوری به‌طور خلاصه مورداشاره قرار گرفته‌اند.

10- Solid State Drive
11- Magnetic Tape Data Storage
12- Compliance Data

جدول۲- مقایسهٔ سیستم بلو-رِی و و راهبرد کتابخانهٔ نوار LTO

ویژگی بررسی‌شده	بلو-رِی با ظرفیت ۱۰۰ GB	نوار مدل LTO-۶ با ظرفیت ۲٫۵ TB	مزیت فناوری نوار
هزینهٔ هر GB	۰٫۶۵ دلار	۰٫۱۹ دلار	نوار بیش از سه‌برابر ارزان‌تر است.
میزان ذخیره‌سازی در هر رک	۱۰۰۰ ترابایت	۲۳۷۵ ترابایت	نوار بیش از دوبرابر جای کمتری می‌گیرد.
سرعت انتقال اطلاعات	۲۷ MB/sec	۱۶۰ MB/sec	نوار بیش از شش‌برابر سریع‌تر است.

انطباق با قواعد صنعتی

بسیاری از کسب‌وکارها به‌منظور تطابق با قواعد صنعتی، به ذخیره‌سازی وُرم روی آورده‌اند. جریمه‌های عدم رعایت قوانین در برخی کشورها سنگین و گاهی تا ۴ میلیون دلار می‌رسد. فناوری، به‌ویژه در حوزهٔ صنعت خدمات مالی، همواره در هنگام نیاز از پس مشکلات برآمده و منابع تازه‌ای برای کسب درآمد یافته است. از طرفی بانک‌ها و شرکت‌های سرمایه‌گذاری باید به‌سراغ وبسایت‌های کاملاً تعاملی با امکان در اختیار گذاشتن اطلاعات بیشتر بروند تا تعاملات خود را از طریق کانال‌های دیجیتال افزایش دهند. برای پاسخ‌دادن به این نیازها و در عین حال مطابقت با قوانین تنظیم‌گری، فناوری وُرم می‌تواند بهترین راهبرد باشد. در پیروی از قوانین تنظیم‌گری که شرکت‌ها را مجاب به سرعت‌بخشیدن به توسعهٔ اپلیکیشن می‌کنند، در اختیار داشتن روشی قابل‌اعتماد برای ذخیره‌سازی ایمن داده‌ها بیشتر از همیشه اهمیت پیدا کرده است.

کاهش خطرات مرتبط با داده‌هایی که به‌صورت مطمئن ذخیره نشده‌اند

برخی از خطراتی که داده‌هایی را که به‌طور مناسب ذخیره نشده‌اند، تهدید می‌کنند عبارتند از:

- هنگامی که افراد غیرمجاز به داده‌هایی دسترسی پیدا می‌کنند که ناامن یا نامناسب ذخیره شده‌اند، ممکن است نقض اطلاعات[۱۳] رخ بدهد.
- اگر داده‌ها به‌درستی ذخیره نشوند ممکن است تصادفاً تخریب شوند و اطلاعات حیاتی از دست برود یا مشکلاتی در تداوم کسب‌وکار بروز یابد.
- اگر داده‌های قدیمی یا تاریخ‌مصرف‌گذشته در فرایندهای تصمیم‌گیری به‌کار گرفته شوند ممکن است باعث مشکل عدم‌انطباق شوند.
- نبود راهبردی مؤثر برای بایگانی اطلاعات ممکن است با رشد حجم داده‌ها به‌مرور زمان به افزایش هزینه‌های ذخیره‌سازی بینجامد.

امنیت بالاتر اطلاعات

اطلاعات داراییِ ارزشمندی است و سازمان‌ها باید برای محافظت از آن در برابر دسترسی‌ها، تغییر یا تخریب غیرمجاز دست به اقداماتی بزنند. یکی از اقدامات به‌کارگیری ذخیره‌ساز وُرم است. وُرم از تغییر یا پاک‌شدن داده‌ها محافظت می‌کند و اطمینان می‌دهد که اطلاعات امن و بدون تغییر باقی می‌مانند. این موضوع به‌ویژه برای داده‌های محرمانه یا حساس اهمیت دارد. به‌علاوه ذخیره‌ساز وُرم از ذخیره‌ساز غیروُرم گزینهٔ قابل‌اعتمادتری است و آن را به انتخابی بهتر برای بایگانی طولانی و حفظ طولانی‌مدت داده‌ها تبدیل می‌کند.

حکمرانی بهتر در حوزهٔ اطلاعات

حکمرانی در حوزهٔ اطلاعات[۱۴] (IG) اعمال سازمان‌دهی، کنترل و تصمیم‌سازی روی اطلاعات است. اجرای IG به سازمان‌ها کمک می‌کند از داده‌های خود محافظت کنند و در همان حال ارزش آنها را بیشینه سازند. حکمرانی اطلاعات در سال‌های اخیر، هم‌زمان با تقلای کسب‌وکارها برای هم‌گامی با رشد انفجاری اطلاعات دیجیتال، اهمیت فزاینده‌ای پیدا کرده است. فواید اصلی به‌کارگیری ذخیره‌ساز وُرم، افزایش سرعت مدیریت اطلاعات حجیم و کاهش خطرات ناشی از شکایت‌های احتمالی یا هزینه‌های حقوقی مرتبط با نقض داده‌های شخصیِ ناشی از خطا در سرورها یا بلایای طبیعی مانند آتش‌سوزی، سیل و از این دست است. ذخیره‌ساز وُرم با کمک به پیروی از مدل مرجع کشف الکترونیکی[۱۵] (EDRM) از اجرای حکمرانی اطلاعات پشتیبانی می‌کند. ذخیره‌سازی وُرم برای کشف الکترونیکی، تحقیقات قانونی و حکمرانی در حوزهٔ اطلاعات ایدئال است.

انواع فناوری وُرم

وُرم سخت‌افزاری

وُرم سخت‌افزاری قدیمی‌ترین روش

13- Data Breach

14- Information Governance

۱۵- Electronic Discovery Reference Model؛ این مدل توسط انجمن وکلای امریکا (ABA) و شرکت‌های فناوری توسعه یافته است و چهارچوبی برای مدیریت اطلاعات ذخیره‌شده به‌صورت الکترونیکی (ESI) در طول چرخهٔ عمر خود، از ایجاد تا تخریب، به‌وجود می‌آورد.

ایجاد رسانهٔ ذخیره‌سازی است که برای اعمال محدودیت نوشتن داده تنها برای یک بار استفاده می‌شود. با توجه به محدودیت‌هایی که وُرم سخت‌افزاری دارد از فناوری PDD[16] که مبتنی بر دیسک‌های نوری و فناوری لیزر آبی است برای ساخت ذخیره‌سازهای مدرن وُرم استفاده می‌شود. ظرفیت ذخیره‌سازی در این فناوری محدود به ۶۰ گیگابایت است. هدف اولیه از سامانهٔ ذخیره‌سازی وُرم، نگهداری ایمن طولانی‌مدت داده‌هاست و برخلاف روش‌های دیگر که بر سرعت و کارآیی تأکید دارند، در این روش هدف جلوگیری از حذف یا تخریب تصادفی داده‌های حساس در طول زمان است. به‌طور کلی به‌خاطر مشکلاتی از جمله عدم‌سازگاری سخت‌افزار و نرم‌افزار و ناتوانی در تضمین صددرصدیِ امنیت داده‌ها به‌دلیل امکان خرابیِ سخت‌افزار یا نرم‌افزاری که سامانه را در برابر دسترسیِ غیرمجاز محافظت می‌کند، وُرم سخت‌افزاری توفیق چندانی پیدا نکرده است.

وُرم نرم‌افزاری

فناوری وُرم نرم‌افزاری به محافظت از فایل‌ها در برابر تغییر یا حذف کمک می‌کند. این فناوری در واقع از یک سامانهٔ نرم‌افزاری ممانعت از نوشتن استفاده می‌کند تا این اطمینان را ایجاد کند که فایلِ در دسترس همان فایلی است که ابتدا ذخیره شده است. این سازوکار از دست‌کاری یا پاک‌شدن غیرمجاز اطلاعات جلوگیری و به رعایت انطباق و همچنین حفظ امنیت داده‌ها کمک می‌کند.

وُرم سیستمی

وُرم سیستمی متشکل از سازوکارهای حفاظتی است که امنیت را با استفاده از میان‌افزارهای کنترل‌کننده یا پردازنده‌های داخلی ایجاد می‌کند. این شیوهٔ پیاده‌سازی وُرم در ذخیره‌سازهای ابری کاربرد دارد و دارای تنظیماتی برای جلوگیری از ویرایش یا پاک‌شدن داده‌هاست که امکانی برای طراحی راهبردهای مختلف برای مدیریت داده‌های ذخیرسازی‌شده در اختیار می‌گذارد.

نتیجه‌گیری

در عصر دیجیتال، سازمان‌ها حجمی نجومی از داده‌ها را تجربه می‌کنند که با سرعتی شگفت‌آور تولید می‌شوند. در همین حال می‌بینیم که داده‌ها در هیئت ارزهای دیجیتال ظاهر می‌شوند و ارزش ذاتی آنها هر روز افزایش می‌یابد. از همین رو محافظت از آنها در برابر تهدیدهای امنیتی و سایر حوادثی که می‌تواند به از دست دادن داده‌ها منجر شود برای تیم‌های امنیتی و مدیریت فناوری اطلاعات اهمیت بیشتری پیدا می‌کند. حصول اطمینان از ماندگاری، اعتبار و درستی داده‌ها برای سازمان‌ها اولویت کلیدی است؛ چراکه باید قوانین تنظیم‌گری و مقرارات تطابق و سایر موافقت‌نامه‌های سطح خدمات را به‌طور دقیق رعایت کنند.

ایجاد پشتیبان‌گیری از داده‌ها برای در اختیار داشتن امکان بازگردانی داده‌های خراب با اطمینان از اصالت آنها معمول است. اما چه خواهد شد اگر نسخهٔ پشتیبان قربانیِ نقض امنیتی شود؟ بنابراین ایجاد سازوکارهای امنیتی مؤثر برای حفاظت از داده‌های ذخیره‌شده، شامل داده‌های اولیه و نسخه‌های پشتیبان، در برابر رخدادهای ناخواسته و پیش‌بینی‌نشدهٔ نقض محرمانگی ضروری است. وُرم به‌عنوان یکی از راهکارهای مؤثر و پذیرفته‌شده برای ایجاد سازوکار حفاظت داده‌ها در این مقاله بررسی شد، اما پرسش نهایی این است که آیا این راهکار ابزاری نهایی و بی‌نقص است یا نیاز به آسیب‌شناسی دارد؟

منابع

- EMC Corp., "EMC Centerra Governance Edition: Content Addressed Storage System," [Online]. Available: http://www.emc.com/products/systems/centera_ce.jsp
- https://www.laserfiche.com/ecmblog/what-is-worm-storage/
- https://www.itproportal.com/blu-ray-vs-tape-which-storage-technology-is-best-for-your-business

16- Professional Disc for Data

نویسنده: محمد قلم‌چی

امنیت سایبری در دنیای امنیت فیزیکی

راهنمایی برای مقابله با تهدیدهای سایبری امروزی و حفاظت از داده‌های حساس در سامانه‌های امنیت فیزیکی

میزان جرایم سایبری همواره در حال افزایش است. بر پایهٔ آنچه سرمایه‌گذاران حوزهٔ امنیت سایبری می‌گویند هزینه‌های ناشی از رخدادهای مجرمانه در این حوزه تا سال ۲۰۲۵ به مرز ۱۰٫۵ تریلیون دلار خواهد رسید. با در نظر گرفتن نرخ رشد ۱۵ درصد در سال، این بزرگ‌ترین جابه‌جایی مالی در تاریخ است. به همین سبب کسب‌وکارها می‌خواهند در برابر این تهدیدهای روبه‌رشد، چابک و توانا واکنش نشان دهند. ایجاد لایه‌های حفاظتی در امنیت به‌عنوان اولین گام خوب است اما احتمالاً کافی نیست. تاب‌آوری واقعی نیازمند راهبردهای تهاجمی بیشتری در حوزهٔ امنیت سایبری است. در همین حال انتخاب شرکای قابل‌اعتمادتری که ابزارهای خودکار کاهش تهدیدها را عرضه می‌کنند ضروری است. در این مقاله مواردی ذکر شده است که به کمک آنها می‌توانید در بازی امنیت سایبری دست بالا را داشته باشید و از کسب‌وکار خود محافظت کنید.

تهدید سایبری چیست؟

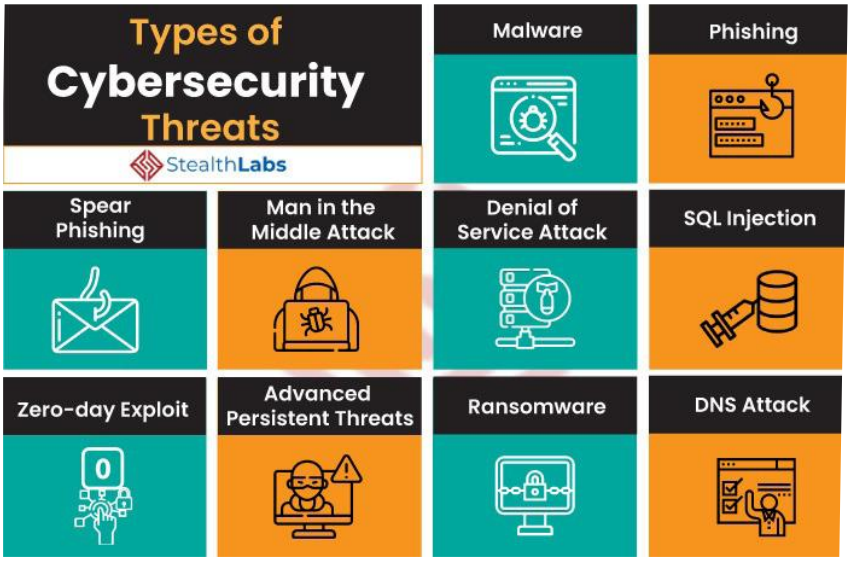
همه در زندگی روزمره با امنیت سایبری سروکار دارند اما در این میان تعهدات صاحبان کسب‌وکار در برابر جامعه مهم‌تر و بیشتر است. به همین سبب باید دربارهٔ حریم خصوصی و امنیت سایبری صریح بود و باور داشت که این دو در کنار هم و نه جدای از یکدیگر می‌توانند منافع بیشتری را به‌همراه داشته باشند.

تهدیدها از کجا نشئت می‌گیرند؟

نفوذ به یک سامانهٔ امنیتی ممکن است از روش‌های گوناگونی انجام شود. امروزه رایج‌ترین روش‌های حمله به سامانه‌های امنیتی را می‌توان به‌صورت زیر دسته‌بندی کرد:

- جاسوس‌افزار[1]: نرم‌افزارهای جاسوسی روی رایانهٔ قربانیان یا ایجاد وب‌سایت‌های تقلبی[2] برای فریب آنها با هدف در اختیار گرفتن اطلاعات مهم شخصی یا سازمانی از قبیل گذرواژه‌ها و اطلاعات کارت‌های اعتباری؛
- باج‌افزار[3]: نرم‌افزارهایی که دسترسی به سامانه یا اطلاعات حیاتی را مسدود می‌کنند تا زمانی که قربانی باجِ خواسته‌شده را به حمله‌کننده بپردازد؛
- حمله‌های به‌منظور اختلال در خدمت‌رسانی[4]: گسیل ترافیک حجیم یا اطلاعات به ماشین یا شبکهٔ هدف به‌گونه‌ای که سبب خرابی و از دسترس خارج شدن آن شود؛
- حمله‌های بروت-فورس[5]: حدس‌زدن گذرواژه‌ها یا استفاده از الگوریتم‌های ساده برای شکستن رمز عبور و به‌دست آوردن دسترسی غیرمجاز به سامانه‌ها یا شبکه‌ها؛
- حمله‌های مرد میانی[6]: استراق‌سمع بسته‌های اطلاعات برای استخراج نام‌های کاربری، گذرواژه‌ها یا داده‌هایی از قبیل محتوای ویدئویی که بر بستر شبکه قرار دارند؛

1- Spyware
2- Copycat Websites
3- Ransomware
4- Distributed Denial of Services
5- Brute-force
6- Man-in-the-middle



– حمله‌های فیشینگ[7]: گسیل اطلاعات جعلی به‌گونه‌ای که به نظر بیایند از یک منبع معتبر فرستاده شده‌اند با هدف فریب به‌منظور افشای اطلاعات حساس یا نصب نرم‌افزارهای مخرب.

حمله‌های سایبری چگونه به اقتصاد یک کسب‌وکار ضربه می‌زنند

رخداد حمله‌های سایبری اگر به‌درستی دفع یا مدیریت نشوند می‌توانند ضربات مهلکی به کسب‌وکارها وارد کنند. نقض اطلاعات[8] ناشی از حمله‌های سایبری، شرکت‌ها و سازمان‌ها را به‌سبب تعهدات قانونی، نظارتی و فنی که برای مقابله و جلوگیری نقض یا افشای اطلاعات دارند با هزینه‌های مالی و پیامدهای حقوقی گوناگونی مواجه می‌کند. هنگامی که شبکه‌ها یا وبسایت‌ها از کار می‌افتند و عملیات مختل می‌شود، بهره‌وری سازمان از دست می‌رود. قربانیان حمله‌های باج‌خواهانه غالباً باید برای بازیابی اطلاعات یا تعویض و تعمیر تجهیزات آسیب‌دیده یا کدهای وبسایت‌های در معرض خطر هزینه کنند. زمانی که داده‌ها نقض می‌شوند مشتریان نیز اعتماد خود را به آن کسب‌وکار از دست می‌دهند و این موضوع برای آن کسب‌وکار ضرر مالی به‌همراه خواهد داشت. ارزش سهام شرکت‌های سهامی عام نیز غالباً بعد از رخداد یک حمله آسیب زیادی می‌بیند. برای اینکه به عمق این تأثیرات پی ببرید بد نیست در اینجا نگاهی آماری به نقل از منابع معتبر و شناخته‌شده به پیامدهای حمله‌های سایبری از جنبه‌های گوناگون بیندازیم.

آی‌بی‌ام در گزارشی با عنوان «هزینه‌های نقض اطلاعات در سال ۲۰۲۲» مدعی شده است که ۱۹ درصد از موارد نقض اطلاعات به دلیل سرقت یا به خطر افتادن اعتبارنامه‌ها در سامانه‌های سایبری و ۱۶ درصد به دلیل حمله‌های فیشینگ رخ داده است. این گزارش همچنین هزینه‌های ناشی از اعتماد ازدست‌رفته را ۱,۴۲ میلیون دلار و هزینهٔ ناشی از نقض اطلاعات را که در سال ۲۰۲۲ به رکورد بالایی رسیده حدود ۴,۳۵ میلیون دلار اعلام کرده است. سایت کامپری‌تک در یک گزارش که آخرین بار در فوریهٔ ۲۰۲۱ به‌روزرسانی‌شده مدعی شده که در طی سه سال ارزش سهام آنها به دلیل نقض سایبری اطلاعات ۳۰,۸ درصد کاهش یافته است. گارتنر هم در گزارش سال ۲۰۲۰ خود پیش‌بینی کرده بود که تا سال ۲۰۲۴، ۷۵ درصد مدیران عامل شخصاً مسئول عواقب رخدادهای امنیتی سایبری خواهند بود. و در نهایت سایت سایبر سکیورتی ونچرز در یک مقاله مدعی شده است که ۶۰ درصد از شرکت‌های کوچک نمی‌توانند کسب‌وکار خود را بیش از شش ماه پس از حملهٔ سایبری حفظ کنند.

توانایی دفاعی امنیت سایبری در سازمان خود را محک بزنید.

فناوری‌های امنیتی قدیمی برای دفاع در برابر حملات امروزی طراحی نشده‌اند و به‌روشنی توانایی پشتیبانی از اصول امنیت سایبری و امنیت شامل محرمانگی، یکپارچگی و دسترس‌پذیری داده‌ها را ندارند. اولین گام برای متناسب‌سازی یا افزایش توانایی دفاع در برابر تهدیدها و حملات شناسایی وضعیت موجود سامانه‌هاست. پرسش‌های زیر اهمیت روزآمدسازی تجهیزات قدیمی حفاظت از امنیت سایبری را خاطرنشان می‌کنند:

– آیا از پیامدهای مالی و عملیاتی رخداد نفوذ و نقض اطلاعات مشتری در صورتی که یکی از صدها دوربین خود را ایمن نکنید آگاهید؟

– آیا از مدت‌زمانی که تیم شما هر ماه صرف به‌روزرسانی نرم‌افزارها و سیستم عامل‌های گوناگون و مدیریت اقدامات امنیت سایبری در سامانه‌های مختلف می‌کند آگاه هستید؟

– آیا توانایی ایجاد و حفظ سیاست‌های ناظر بر گذرواژه‌های قوی و محدودکردن مؤثر دسترسی به داده‌های سازمان را دارید؟ آیا می‌توانید امکان ورود به سامانه‌ها را از ورود تک‌مرحله‌ای به اعتبارسنجی چندلایه تغییر دهید؟

– آیا سامانه‌های شما این امکان را دارند که تازه‌ترین روش‌های

7- Phishing
8- Data Breach

رمزگذاری یا ویژگی‌های امنیت سایبری را پیش از رخداد تهدیدات در حال تکامل به‌کار بگیرید؟

- آیا اگر سازمان شما با تقاضایی از سوی مشتری یا نیروی امنیتی مبنی بر تقاضای دسترسی به فیلم‌های ضبط‌شده مواجه شد، می‌توانید با حفظ هویت سایر افراد فیلم‌ها را در اختیار درخواست‌کنندگان بگذارید؟

تقویت تدبیرهای حفاظت از داده‌ها

در بخش پیش دیدیم که چگونه می‌توان از میزان آمادگی سامانه‌های دفاعی و امنیتی سایبری سازمان مطلع شد و به برآورد مناسبی از لزوم اندیشیدن و استقرار تدابیر جدید و یا افزایش توانمندی تدابیر مستقر و فعال فعلی دست یافت. در ادامه به گام بعدی اشاره می‌کنیم.

سه لایهٔ بسیار مهم در امنیت سایبری

امروزه می‌توان برای ایجاد تاب‌آوری در استقرار امنیت فیزیکی در برابر تهدیدات سایبری، کارهای گوناگونی انجام داد. چندلایه کردن امنیت یکی از این کارها و شاید مهم‌ترین آنهاست. هرچه لایه‌های امنیتی بیشتری ایجاد کنید کسب‌وکار شما بیشتر محافظت می‌شود. در ادامه به برخی از این تدابیر نگاهی می‌اندازیم.

لایهٔ اول: رمزنگاری

به زبان ساده، رمزنگاری به حفاظت از تمام داده‌های سامانه‌های امنیت فیزیکی که توسط تجهیزات امنیتی از قبیل دوربین‌های نظارتی، کنترل دسترسی و دیگر سنسورهای IOT که از سرورها یا ایستگاه‌های کاری سرویس‌گیرنده دریافت یا به آنها ارسال می‌شود، کمک می‌کند. این کار با رمزگذاری اطلاعات یا درهم‌ریختن متون قابل‌خواندن برای پنهان‌سازی و محافظت آنها از دسترسی‌های غیرمجاز قابل‌انجام است.

البته وقتی به‌طور خاص، رمزنگاری تصاویر حاصل از دوربین‌های نظارتی مطرح است باید از روش‌های رمزگذاری قوی هم برای داده‌های در حال انتقال و هم برای داده‌های ایستا بهره جست، هرچند داده‌های در حال انتقال آسیب‌پذیرتر هستند و عوامل تهدید همیشه ضعیف‌ترین نقطه را هدف قرار می‌دهند.

لایهٔ دوم: احراز هویت

احراز هویت فرایندی است که هویت کاربر، سرور یا برنامهٔ کاربردی سرویس‌گیرنده را پیش از اعطای مجوز دسترسی به منابع محافظت‌شده تأیید می‌کند. احراز هویت در سمت سرویس‌گیرنده با روش‌های گوناگونی از جمله نام کاربری و گذرواژه یا نشانهٔ امنیتی انجام می‌شود. تأیید اشخاص ثالث در سمت سرور، معمولاً از طریق گواهی‌های دیجیتال صورت می‌گیرد.

استقرار چندگانهٔ سازوکارهای احراز هویت، امنیت بیشتری را به‌دنبال دارد و به همین سبب، فراتر از گذرواژه، باید از احراز تلفنی، بیومتریک یا نشانه‌های امنیتی[9] سخت‌افزاری و یا کارت هوشمند یا سایر سازوکارهای دفاعی در برابر عوامل تهدید بهره جست.

لایهٔ سوم: صدور مجوز

صدور مجوز فرایندی است که امکان تعریف سطوح دسترسی خاص برای کاربران و ایجاد محدودیت در دسترسی به اطلاعات و منابع سامانه را در اختیار مدیران قرار می‌دهد. صدور مجوز در سامانهٔ امنیتی می‌تواند دربرگیرندهٔ محدودیت‌هایی از جمله زمان دسترسی، گروه اطلاعات قابل‌دسترسی، امکان به اشتراک گذاشتن اطلاعات و منابع و مدت‌زمان نگهداری داده‌ها هم بشود.

اقدامات تکمیلی

علاوه بر این تدابیرها، رویکردهای اطمینان‌بخشی نیز وجود دارند که کارایی تمهیدات پیش‌گفته را برای رسیدن به امنیت سایبری دوچندان می‌کنند که در ادامه به برخی از آنها اشاره می‌شود:

- اطلاعات را دور از دسترس نگه دارید:
  برای محافظت از داده‌های خود و جلوگیری از سرقت آنها به‌دست افراد غیرمجاز به روش‌های پیشرفتهٔ

9- Security token

رمزگذاری، صدور مجوز و احراز هویت تکیه کنید. مثلاً در سامانه‌های نظارت تصویری، با استفاده از ویژگی‌های واترمارک و امضای دیجیتال، همواره از اصالت تصاویر ضبط‌شده و عدم دست‌کاری آنها از سوی کاربران غیرمجاز اطمینان حاصل می‌شود.

- اطمینان پیدا کنید که داده‌ها همیشه دسترس‌پذیر هستند: امکان بازیابی پس از فاجعه را پیاده‌سازی کنید، وضعیت امنیت سایبری خود را به‌طور مداوم و بلادرنگ رصد کنید و برای دستیابی به تاب‌آوری، توصیه‌نامه‌ها را به‌کار بگیرید. همهٔ این موارد به شما کمک می‌کنند که مطمئن شوید داده‌های شما همیشه دسترس‌پذیر هستند و همهٔ اجزای سامانه همان‌طور که باید کار می‌کنند.
- از نرم‌افزارها و تجهیزات خود نگهداری و مراقبت کنید: نگهداری، به‌روزرسانی و نظارت توکار سلامت[10] کارایی سامانهٔ شما را در پیشینهٔ خود حفظ می‌کند. این امکان وجود دارد که به‌روزرسانی نرم‌افزارها و میان‌افزارها را به‌طور متمرکز برنامه‌ریزی و تغییر گذرواژه‌ها را خودکار کنید تا آسیب‌پذیری‌های احتمالی به‌سرعت رفع شوند.
- سامانهٔ خود را ممیزی و فعالیت‌های کاربران را رصد کنید: با تعبیهٔ توالی‌های ممیزی توکار[11] و استفاده از گزارش‌های فعالیت کاربران یک زنجیرهٔ کامل نگهداری ایجاد کنید. با ساده‌سازی فرایند شناسایی هویت و برنامه‌ریزی بازبینی سطوح دسترسی الزامات ممیزی و سیاست‌های سازمان را رعایت کنید.
- به راهکارهای آزموده‌شده و سازگار تکیه کنید: به راهکارهایی که یکپارچگی داده‌اند و جواب داده‌اند، اعتماد کنید. استانداردها را جدی بگیرید و آزمون‌های نفوذ را اجرا کنید.
- یکپارچه‌سازی راه آسان‌تر و مؤثرتری برای محافظت از داده‌ها فراهم می‌کند: بسیاری از سازمان‌ها برای مقابله با هکرها و محافظت از کسب‌وکار خود به‌دنبال راهبردی واحد و عمومی برای محافظت از داده‌ها و حفظ حریم خصوصی هستند. وجود یک مرکز امنیتی استاندارد که شیوه‌های امنیت سایبری را به‌صورت یکپارچه در سامانهٔ فیزیکی اجرا کند، این فرایند را تسهیل می‌کند. برای روشن‌شدن موضوع موارد زیر را مرور کنید:

* حفاظت از داده‌ها را متمرکز کند: با استفاده از یک پلتفرم یکپارچه، می‌توانید از طریق یک رابط یکتا کنترل داده‌ها را به‌دست بگیرید و لازم نیست زمانی را برای بررسی راه‌های گوناگون آزمودن سلامت سایبری سامانهٔ خود تلف کنید.
* بسیاری از اقدامات دفاعی داخلی را توکار کند: ابزارها و خدمات یکپارچه، شما را از آسیب‌پذیری‌های احتمالی آگاه می‌سازند و عملیات به‌روزرسانی را ساده می‌کنند.
* با منحصرکردن ورود به سامانه به یک بار لاگین، خطرات را کاهش دهد: با یک پلتفرم یکپارچه، کاربران شما با یک گذرواژه به همهٔ منابعی که جوازش را دارند دسترسی پیدا می‌کنند. این امر احتمال سرقت یا هک‌شدن چندین گذرواژه و احتمال نقض اطلاعات را کمینه می‌کند. همچنین این امکان وجود دارد که سیاست‌های نگهداری داده را در سراسر سامانهٔ خود بر پایهٔ قوانین محلی سفارشی کنید.

تأمین‌کنندگان خود را محک بزنید

یکی از بهترین روش‌ها برای کاهش ریسک انتخاب تأمین‌کنندگان معتبر، فناوری است. اگرچه این روزها همهٔ تأمین‌کنندگان مدعی هستند که در تولید و عرضهٔ ملزومات فناوری اطلاعات، امنیت سایبری را به‌طور کامل در نظر دارند، اما برای ارزیابی قابلیت اعتماد به این ادعا در زنجیرهٔ تأمین بهتر است از چک‌لیست زیر کمک بگیریم:

- آیا تأمین‌کننده به‌طور مستمر و فعال ظهور تهدیدهای تازه و پیامدهای احتمالی آنها بر عملیات، داده‌ها و افراد را زیر نظر دارد؟
- آیا راهبرد جامعی برای پرکردن شکاف‌ها و آسیب‌پذیری‌های امنیتی دارد؟
- چه سیاست‌هایی در برابر نگرانی‌های امنیت سایبری دارد؟
- آیا راهکارهای ارائه‌شده توسط آنها شامل امنیت چندلایه، متشکل از فناوری‌های پیشرفته، احراز هویت و فناوری‌های رمزگذاری است؟
- آنها چگونه از داده‌های سازمان و حریم خصوصی مشتریان حفاظت می‌کنند؟
- آیا شرکای آنها هم امنیت و حفاظت از داده‌ها را در نظر دارند؟ آیا شرکای خود را به‌گونه‌ای با دقت انتخاب می‌کنند که

10- Built-in health monitoring

11- Built-in audit trails

بالاترین سطح امنیت و انطباق وجود داشته باشد؟

- چه اقداماتی برای آگاه‌سازی و پشتیبانی از مشتریان خود با نگاه به بهترین تجارب امنیت سایبری انجام می‌دهند؟
- آیا آمادهٔ مواجهه با آسیب‌پذیری‌های شناخته‌شده در آینده هستند و برای رفع سریع مشکل راهبردی در اختیار می‌گذارند؟
- آیا به استانداردهای امنیت اطلاعات مانند ایزو ۲۷۰۰۱ پایبند هستند؟ آیا دارای گواهی‌نامه‌های لازم از نهادهای نظارتی هستند؟
- آیا از ممیزهای حرفه‌ای برای اجرای آزمایش‌های نفوذ و شناسایی و رفع حفره‌های امنیتی بهره می‌جویند؟

افزایش امنیت سایبری با راهکارهای ابری و ابر هیبریدی

استقرار امنیت فیزیکی در سازمان در حالی که سعی در به‌کارگیری بهترین شیوه‌های امنیت سایبری می‌شود نیازمند اقدامات زیادی روی سامانه‌ها و تجهیزات نصب‌شده در محل است. وقتی حرف از امنیت فضاهای مختلف باشد، پیچیدگی این موضوع سر به فلک می‌کشد. خدمات ابری از آن رو که بار نگهداری مستمر را از دوش تیم فناوری اطلاعات و امنیت برمی‌دارند راه ساده‌تری برای رسیدن به تاب‌آوری سایبری در اختیار می‌گذارند. برای درک بهتر به موارد زیر نگاهی بیندازیم:

دسترسی به آخرین امکانات امنیت سایبری

با استفاده از راه‌حل‌های امنیت فیزیکی که بر پایهٔ فناوری ابری پیاده‌سازی شده‌اند همیشه به آخرین امکانات و ویژگی‌های توکار امنیت سایبری از جمله ارتباطات رمزنگاری‌شده، حفظ حریم خصوصی، احراز هویت قوی و انواع ابزارهای پایش سلامت سامانه دسترسی خواهیم داشت.

دریافت آنی به‌روزرسانی‌ها و افزونه‌های امنیتی

با استفاده از خدمات ابری به‌محض انتشار آخرین نسخه، به‌روزرسانی‌ها آن را دریافت خواهید کرد. بدین ترتیب می‌توانید مطمئن باشید سامانه‌های امنیت فیزیکی شما همیشه به‌روز هستند و در برابر آسیب‌پذیری محافظت می‌شوند.

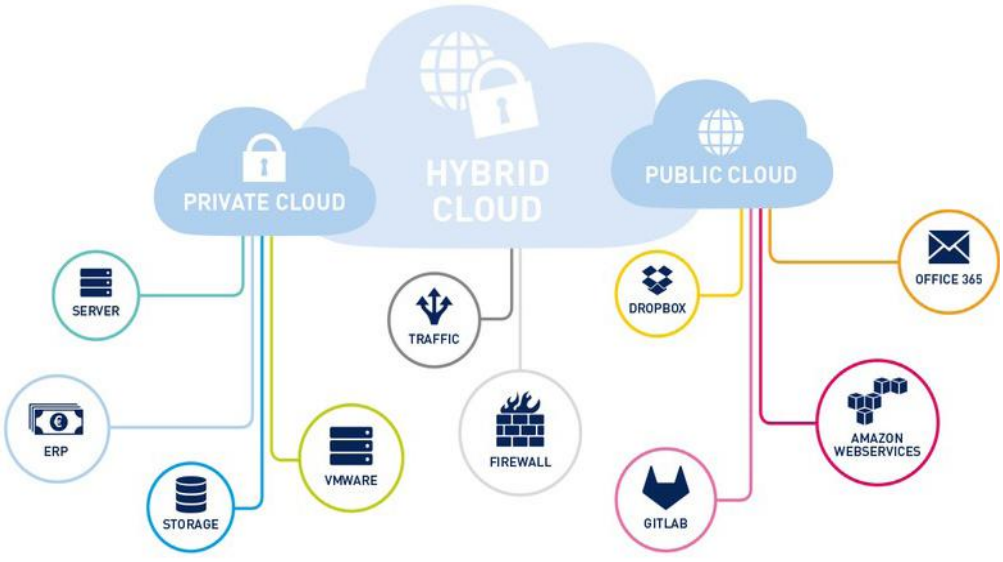
افزایش افزونگی داده‌ها

وقتی از روش پیاده‌سازی ابر هیبریدی برای پیاده‌سازی سامانهٔ امنیت فیزیکی استفاده کنید، افزونگی در سامانه را افزایش می‌دهید. به این معنی که یک سامانهٔ امنیتی کامل در محل و مخزن ذخیره‌ساز تصاویر در فضای ابری قرار دارند و می‌توانید نسخه‌های متعددی از تصاویر را در فضای ابری نگهداری کنید و با ایجاد افزونگی به سطح بالاتری از اطمینان و دسترس‌پذیری برسید.

چگونه راهبرد امنیت سایبری خود را مؤثر نگه داریم

حفظ امنیت سایبری در سامانهٔ امنیت فیزیکی فقط به معنی دفاع در برابر حملات نیست. بلکه به معنی ایجاد اعتماد نزد مشتریان و شرکا و تضمین تداوم موفقیت کسب‌وکار شما نیز هست. برای انجام درست این اقدام باید به‌طور مداوم اقدامات حفاظت از داده‌ها و حریم خصوصی ارزیابی شوند. در ادامه به چگونگی این موارد اشاره شده است:

- از چشم‌انداز تهدیدها آگاه باشید: منتظر دیگران نمانید تا شما را از تهدیدهای سایبری آگاه کنند. تمام تلاش خود را به‌کار ببندید تا پابه‌پای تحولات در حوزهٔ تهدیدها و راهبردهای کاهش آسیب‌ها پیش بروید و آنگاه بایدها و نبایدها را به کارکنان خود آموزش دهید.
- برای ارزیابی ریسک و کشف دارایی اقدام کنید: ریزه‌کاری‌های اطراف خود را بشناسید تا بتوانید سازوکارهای امنیت سایبری را درست پیاده‌سازی کنید. فهرستی از رایانه‌ها، ادوات اینترنت اشیا، کاربران، نوع داده‌ها و از این قبیل موارد تهیه کنید. این اقدام به شما کمک می‌کند تا سطوح بالاتری‌ازامنیت‌سایبری‌راحفظ‌کنید.
- حواستان به تمام به‌روزرسانی‌ها و افزونه‌های امنیتی باشد: افزونه‌های نرم‌افزاری به‌ویژه در مواجهه با آسیب‌پذیری‌های امنیتی و کاهش خطرات احتمالی بزرگ به شما کمک می‌کنند. فرض کنید ابزار خودکار به شما در مورد به‌روزرسانی نرم‌افزار یا سیستم هشدار می‌دهد، در این صورت هرگز فرصت نفوذناپذیر نگه داشتن سامانهٔ امنیت فیزیکی خود را از دست نمی‌دهید.
- پیاده‌سازی احراز هویت چندعاملی را آغاز کنید: تنها به گذرواژه‌ها متکی نباشید چراکه ممکن است به‌راحتی سرقت یا دست‌به‌دست



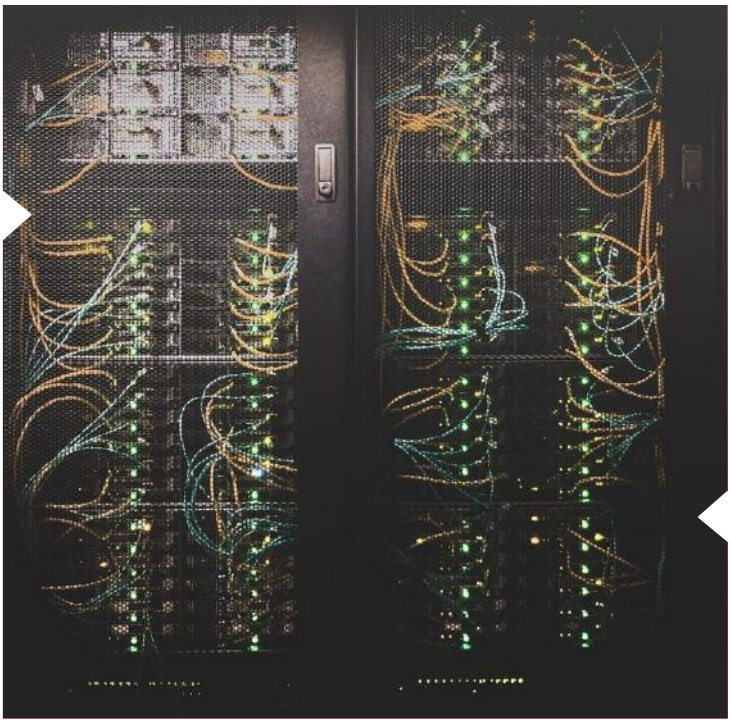
شوند. امروزه، حفاظت واقعی در برابر تهدیدهای سایبری نیازمند بهره جستن از روش‌های گوناگون احراز هویت به‌طور هم‌زمان است. راجع به استفاده از گذرواژه‌ها مطمئن شوید که به‌صورت دوره‌ای توسط کاربران مجاز یا مدیران سامانه تغییر داده می‌شوند.

– راه‌های نفوذ را مسدود کنید: هدف شما از تمام تمهیدات امنیتی، رسیدن به محافظت صددرصدی است و لی با این حال ممکن است این تلاش‌ها برای دور نگه داشتن مهاجمان کافی نباشد. در اختیار داشتن یک سامانهٔ امنیتی فیزیکی که خطرات احتمالی را تشخیص دهد ضروری است اما در کنار آن حتماً باید برنامه‌ای برای واکنش نشان دادن به رخنه‌ها و حوادث امنیتی نیز داشته باشید.

نتیجه‌گیری

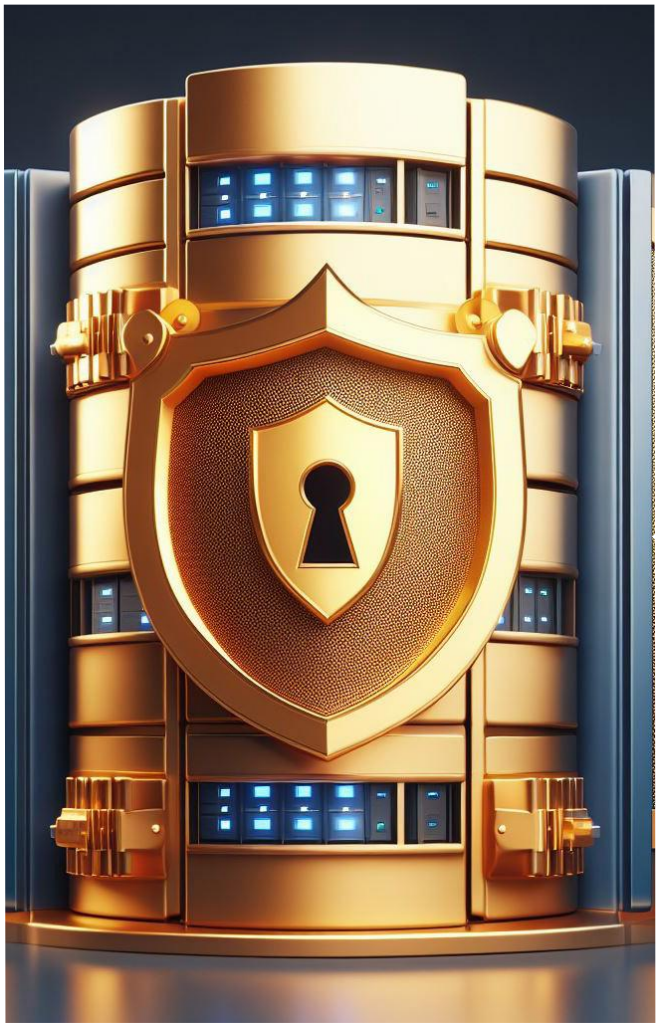
شیوه‌های حمله و تهدید بالقوهٔ سایبری هر سال پیچیده‌تر می‌شوند و این موضوع بر سازمان‌ها و کسب‌وکارها فشار می‌آورد تا استانداردهای مربوطه را ارتقا دهند و گواهینامه‌های جدیدی اخذ کنند. گسترهٔ این امر اغلب از ملاحظه‌های امنیتی راجع به سامانه‌های امنیت فیزیکی فراتر می‌رود و به‌کل اکوسیستم زنجیرهٔ تأمین نیز تسری می‌یابد؛ زیرا آنچه در سال گذشته برای امنیت داده‌ها مفید بوده، ممکن است برای دور نگه داشتن یا مقابله با عوامل تهدید فعلی کافی نباشد.

وقتی نوبت به بهترین شیوه‌های امنیت سایبری می‌رسد، اولین گام آگاهی است. لازم است همهٔ بایدها و نبایدها و پیامدهای اقدامات خود را بدانید. کسب‌وکارها به یک برنامهٔ واکنشی قوی در رابطه با حوادث نیاز دارند؛ زیرا فارغ از اینکه کنش دفاعی در برابر تهدید چقدر خوب باشد، احتمال وقوع حادثه وجود دارد. باید اطمینان حاصل شود که در صورت بروز حادثه، امکان حفاظت و بازیابی داده‌ها و دارایی‌های سازمان در سریع‌ترین زمان ممکن وجود دارد. راهکارهای سازگار و مقاوم برای مراقبت از سامانه‌های سایبری، سامانه‌های امنیت فیزیکی سازمان شما را نیز ایمن و قابل‌اتکا خواهد کرد. البته این پایان راه نیست.



منابع

– https://cybersecurityventures.comhackerpocalypse-cybercrime-report
– https://www.ibm.com/security/data-breach
– https://www.comparitech.com/blog/information-security/data-breach-share-price/
– https://www.gartner.com/en/newsroom/press-releases/gartner-predicts-of-ceos-will-be-personally-liabl
– https://cybersecurityventures.com/percent-of-small-companies-close-within-months-of-being-hacked



حاکمیت اطلاعات:
تعاریف و مفاهیم

نویسنده: مصطفا کردی

اطلاعات و بزرگی حجم آن سوخت تحول دیجیتالی است که در همه‌ی صنایع در حال رخ دادن است. در همان حالی که سازمان‌ها محصولات، کانال‌ها و عملیات جدیدی را توسعه می‌دهند برای تصمیم‌گیری‌های راهـبردی به اطلاعات گسترده‌تری نیاز دارند.

ایـن تغییـر و تحـول، پیچیدگـی روبه‌تزایـد دارایی‌هـا، الزامـات تـازه‌ای بـرای تنظیم‌گـری، افزایـش انتظـارات مشـتری بـرای حفـظ حریـم خصوصـی و نیـاز شـدید بـه رقابتـی مانـدن را به‌همـراه دارد. اطلاعـات و داده‌هـا منابـع ارزشـمندی هسـتند کـه در دهـهٔ گذشـته ارزشـی چـون طـلا پیـدا کرده‌انـد. در عصـر اینترنـت، اطلاعـات و داده‌هـا را می‌تـوان از رسـانه‌های اجتماعـی، وب‌سـایت‌ها، نشـریه‌ها و هـر منبـع حـاوی اطلاعـات تحلیلـی اسـتخراج کـرد. اطلاعـات و داده‌هـا می‌تواننـد بـرای مقاصـد قانونـی یـا غیرقانونـی توسـط افـراد، گروه‌هـا یـا دولت‌هـا بـه‌کار گرفتـه شـوند. اجـرای اصـول حاکمیـت اطلاعـات در یـک سـازمان یـا پـروژهٔ فنـاوری اطلاعـات ضـروری اسـت. ایـن اقـدام می‌توانـد از دسترسـی غیرقانونـی جلوگیـری کنـد، ریسـک را کمینـه نمایـد، کیفیـت داده‌هـا را بـالا ببـرد و کارایـی در مدیریـت اطلاعـات و داده‌هـا را افزایـش دهـد.

پیـش از آنکـه دربـارهٔ حاکمیـت اطلاعـات و چگونگـی و چرایـی دشـواری پیاده‌سـازی آن بنویسـیم بایـد روشـن کنیـم کـه منظـور از «حاکمیـت اطلاعـات» چیسـت. درسـت ماننـد اصطـلاح «اطلاعـات» کـه وقتـی افـراد مختلـف دربـارهٔ آن حـرف می‌زننـد معناهـای متفاوتـی را در نظـر دارنـد. تعاریـف بسـیاری بـرای «اطلاعـات» وجـود دارد کـه هیچ‌یـک از آنهـا به‌صـورت عمومـی پذیرفتـه نشـده‌اند و به‌تبـع آن ایـن اختلافـات بـرای اصطلاحاتـی چـون «حاکمیـت»، «داده»، «دانـش» و حتـی «محتـوا» نیـز وجـود دارد. هرچنـد صحبـت از کلیـت ایـدهٔ «حاکمیـت اطلاعـات» سـاده‌تر اسـت، امـا چنیـن رویکـردی ممکـن اسـت محـدودهٔ ایـن ایـده را تنـگ و جزئیـات مهمـی را از چشـم پنهـان سـازد. بـه همیـن سـبب تـلاش می‌کنیـم در ایـن نوشـته ابتـدا اطلاعـات و سـامانهٔ اطلاعاتـی را کـه بـه نوعـی ارکان اصلـی یـک زیسـت‌بوم مبتنـی بـر اطلاعـات هسـتند به‌طـور خلاصـه بررسـی کنیـم و آنـگاه به‌سـراغ مفهـوم حاکمیـت و سـپس حاکمیـت اطلاعـات برویـم.

اطلاعات

اطلاعـات دانـش ارزشـمندی اسـت کـه از مجموعـه‌ای از داده‌هـا تولیـد می‌شـود. بـر پایـهٔ تعریـف مـک فـادن[1]، اطلاعـات داده‌هایـی هسـتند کـه بـه دانشـی تبدیـل شـده‌اند کـه بـرای فـردی کـه از داده‌هـا اسـتفاده می‌کنـد، ارزشـمند هسـتند. اطلاعـات زمانـی می‌تواننـد مفیـد باشـند کـه قابل‌فهـم شـوند و بتـوان از آنهـا در تصمیم‌سـازی‌ها اسـتفاده کـرد. سـطح اطلاعـات مفیـد بـا سـطح کیفیـت اطلاعـات سـنجیده می‌شـود. به‌دنبـال محبوبیـت اطلاعـات در عصـر اینترنـت، کیفیـت اطلاعـات بـه نگرانـی تـازه‌ای تبدیـل شـده اسـت. کیفیـت اطلاعـات بـه جنبه‌هایـی مانـده دقـت، بـه‌روز بـودن، سـازماندهی خـوب و قابل‌اسـتفاده بـودن اشـاره دارد. ایـن بـه آن معنـی اسـت کـه بیـش از یـک عامـل در تعییـن کیفیـت اطلاعـات مؤثـر اسـت.

سامانهٔ اطلاعاتی

سـامانهٔ اطلاعاتـی، سـامانه‌ای متشـکل از زیرسـامانه‌های متصل‌به‌هـم اسـت کـه بـرای مدیریـت و فـراوری داده‌هـا بـه اطلاعـات ارزشـمند توسـعه یافتـه اسـت. بنـا بـر گفتـهٔ دیویـس و یِـن[2]، سـامانهٔ اطلاعاتـی شـامل اجزایـی ماننـد انسـان، سـخت‌افزار، نرم‌افـزار و داده اسـت و وظیفـهٔ آن فراهـم کـردن اطلاعـات و داده بـرای کاربـر موردنظـر اسـت. اسـتفاده از سـامانه‌های اطلاعاتـی در سـازمان‌ها بـا فراگیـر شـدن اینترنـت به‌سـرعت افزایـش یافتـه اسـت. بـا ایـن حـال توسـعهٔ یـک سـامانهٔ اطلاعاتـی موفـق بـه اقدامـات پیچیـده‌ای نیـاز دارد. جوانـب بسـیاری بایـد بـا دقـت در نظـر گرفتـه شـوند. بـر اسـاس مـدل دِلـون و مک‌لیـن[3]، شـش معیـار بـرای ارزیابـی یـک سـامانهٔ اطلاعاتـی موفـق وجـود دارد کـه عبارتنـد از: کیفیـت اطلاعـات، کیفیـت سـامانه، کیفیـت خدمـات، کاربـرد سـامانه، رضایـت کاربـر و منافـع کلـی.

بـر پایـهٔ مـدل دلـون و مک‌لیـن کـه شـمای آن در شـکل ۱ آمـده اسـت، تولیـد یـک سـامانهٔ اطلاعاتـی موفـق نیازمنـد دقـت در جوانـب گوناگونـی نظیـر مدیریـت زمـان و میانگیـن رضایـت از دیـدگاه کاربـر بـرای تحقـق معیارهـای پیش‌گفتـه اسـت. همچنیـن بـرای سـنجش کیفیـت سـامانه بایـد بـه سـاعات عملیاتـی و دسـترس‌پذیری توجـه داشـت، بـرای کیفیـت اطلاعـات بـه میـزان دقـت و مرتبـط بـودن داده‌هـا، بـرای سـنجش کیفیـت خدمـات بـه دسـترس‌پذیری و قابلیـت اطمینـان خدمـات و بـرای سـنجش بهـره‌وری و منفعـت کلـی بـه دفعـات اسـتفاده از سـامانه و پشـتیبانی فنـی کاربـری سـامانه.

حاکمیت

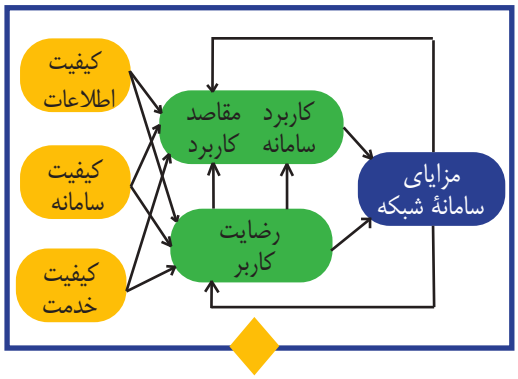
مفهـوم حاکمیـت قدمتـی بـه انـدازهٔ اولیـن سـازمان ایجادشـده توسـط انسـان دارد. ایـن مفهـوم به‌خودی‌خـود بـه شـیوهٔ هدایـت سـازمان اشـاره دارد. حاکمیـت ماننـد همـهٔ اندیشـه‌ها هـم محصـول تاریـخ اسـت و هـم مولـد تاریـخ. حاکمیـت را هـم بایـد به‌عنـوان یـک هنجـار و هـم به‌صـورت یـک کنـش در نظـر گرفـت. حاکمیـت چـه به‌عنـوان یـک اندیشـه و چـه به‌عنـوان یـک نهـاد در قلـب دولـت مـدرن جـا دارد. توسـعهٔ مفهـوم حاکمیـت و قابلیـت و کاربـرد آن بـه تقسـیم قـدرت بیـن دولـت و جامعـه بسـتگی دارد. متخصصـان علـم مدیریـت حاکمیـت را مجموعـه‌ای از روش‌هـا و مقـررات و سـاختارها بـرای ادارهٔ قلمـروی بـا حـدود مشـخص تعریـف می‌کننـد.

گرچه مفهوم حاکمیت جدید نیست، امروزه ما این مفهوم را تحت عناوینی چون حاکمیت شرکتی، حاکمیت سازمانی و حاکمیت خوب

1- McFadden

2- W. S. Davis and D. C. Yen

3- DeLone and McLean



شکل ۱- مدل دلون و مک‌لین

می‌شنویم. در واقع حاکمیت شرکتی یا آنچه در ایزو ۲۶۰۰۰ تعریف شده، سامانه‌ای است که سازمان با استفاده از آن برای تعقیب اهداف خود تصمیم‌گیری می‌کند. به‌طور ساده حاکمیت به‌معنای فرایند تصمیم‌گیری و فرایندی است که به‌وسیلهٔ آن تصمیمی عملی می‌شود (یا نمی‌شود) و بر اساس همین استاندارد، حاکمیت مهم‌ترین عامل در توانمندسازی سازمان برای پذیرفتن مسئولیت تأثیر تصمیمات و اقدامات خود می‌باشد.

عناصر حاکمیت

مؤسسهٔ OCEG در سال ۲۰۰۹ حاکمیت را چنین تعریف کرد: حاکمیت عبارت است از فرهنگ، ارزش‌ها، مأموریت، ساختار، لایه‌های سیاست (خط‌مشی‌ها)، فرایندها و مقیاس‌هایی که سازمان با استفاده از آنها مدیریت و کنترل می‌شود. بر اساس این تعریف یکی از مهم‌ترین مسئولیت‌های حاکمیت فراهم کردن راهنمایی است که به خط‌مشی ترجمه شود. حاکمیت معمولاً به ساختاری سلسله‌مراتبی از خطوط راهنما، خط‌مشی‌ها، مسئولیت‌ها و رویه‌ها گفته می‌شود که تضمین می‌کند سطح مشخصی از کنترل در سازمان در حال اجراست. حاکمیت از استراتژی، اهداف، خط‌مشی‌ها، رویه‌ها، ساختار و فرایند تشکیل شده است.

حاکمیت اطلاعات

از نظر گارتنر، حاکمیت اطلاعات چهارچوبی برای مدیریت اطلاعات با رفتاری مناسب است. گارتنر حاکمیت اطلاعات را به‌عنوان مشخصهٔ حقوق تصمیم‌گیری و چهارچوب پاسخ‌گویی برای اطمینان از رفتار مناسب در ارزش‌گذاری، ایجاد، ذخیره‌سازی، بهره‌برداری، بایگانی و پاک کردن اطلاعات تعریف می‌کند. این [چهارچوب] شامل فرایندها، نقش‌ها و سیاست‌ها، استانداردها و سنجه‌هایی است که کاربرد مؤثر و کارآمد اطلاعات در توانمندسازی سازمان برای دستیابی به اهداف خود را تضمین می‌کند. حاکمیت اطلاعات تنها جنبه‌های فنی ندارد بلکه شامل جنبه‌های اجتماعی هم می‌شود. ارائهٔ یک حاکمیت اطلاعات خوب بر سه پایه استوار است: پشتیبانی از کیفیت و قابل‌اتکا بودن اطلاعات، امکان ادغام، اعتبارسنجی و تأیید و در نهایت وجود بستر تحلیل و تصمیم‌سازی. در عصر شبکه‌های اجتماعی، حاکمیت اطلاعات نقش مهمی در آگاه‌سازی افراد یک سازمان در حوزهٔ مدیریت اطلاعات و داده‌ها ایفا می‌کند. لوماس و همکارانش ادعا می‌کنند که حاکمیت اطلاعات به‌عنوان چهارچوب اخلاقی کل‌نگر تعریف می‌شود که فرایند به‌اشتراک‌گذاری، مدیریت، همکاری در خلق، مالکیت و حقوق اطلاعات را امکان‌پذیر می‌کند. این ادعا با عبارت وبر[4] که می‌گوید حاکمیت اطلاعات، اقدامات ساختاری، اقدامات رویه‌ای، مسئولیت‌های فردی و اقدامات مبتنی بر روابط را شامل می‌شود هم‌خوانی دارد.

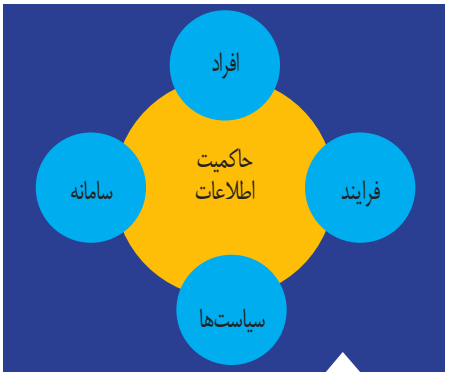
بر اساس ادعای اسمال‌وود[5]، پیاده‌سازی حاکمیت اطلاعات می‌تواند الزامی قانونی برای این باشد که سازمان‌ها [توجیهاتی] چون اطلاعات بی‌استفاده، امنیت خصوصی، حفاظت از اطلاعات حساس و مدیریت اطلاعات محرمانه را کنار بگذارند. مزیت دیگر حاکمیت اطلاعات، فراهم کردن یک روش مدیریت مطمئن و استوار، امنیت، بهینه‌سازی و کنترل اطلاعات است. ده دلیل برای پیاده‌سازی حاکمیت اطلاعات در یک سازمان وجود دارد:

- توانمندسازی سازمان‌ها برای دور ریختن اطلاعات غیرضروری
- فراهم کردن چهارچوبی برای تصمیم‌گیری دربارهٔ ضروری بودن یا نبودن اطلاعات
- آسان‌کردن فرایند یافتن اطلاعات و تولید اطلاعات پاسخ‌گو
- تمرکز بر اطلاعات ارزشمند، بهبود تحویل اطلاعات و بهبود بهره‌وری
- ارائهٔ روشی برای پاسخ‌گویی به تغییرات آیین‌نامه‌ها و فناوری
- شناسایی و مدیریت ریسک
- کمک به کنترل ایمیل
- رعایت محرمانگی
- در نظر گرفتن اطلاعات به‌مثابهٔ دارایی
- کمک به ممیزی یا بررسی فرایندها

مدل‌های استقرار حاکمیت اطلاعات در سازمان‌ها

راهبران امنیت اطلاعات و حفظ حریم شخصی باید مدل درستی را برای حاکمیت اطلاعات در سازمان متبوع خود برگزینند تا بتوانند به اهداف خود برسند.

گارتنر در پویشی که در سال ۲۰۲۱ انجام شد به این نتیجه رسید که تقریباً دوسوم از دست‌اندرکاران حفظ امنیت اطلاعات و حریم شخصی یعنی چیزی حدود ۶۳٪ با ضرورت و فوریت حاکمیت اطلاعات برای سال ۲۰۲۲ موافق بودند ولی فقط از ۶٪ از فرایندهای فعلی سازمان خود رضایت دارند. اولین پرسش در مسیر توسعهٔ حاکمیت اطلاعات این است که «چگونه باید ساختارمند شویم؟»



شکل ۲- اجزای حاکمیت اطلاعات

4- K. Weber

5- R. F. Smallwood

هرچند نمی‌توان پاسخی دقیق به این پرسش داد ولی تردیدی نیست که باید مناسب‌ترین مدل را از بین مدل‌های مختلف برای هر سازمان انتخاب کرد. گارتنر طی پویشی که ذکرش در سطور پیش رفت آشکار کرد که سازمان‌ها در چهارچوب یکی از مدل‌های سه‌گانهٔ زیر به‌سوی حاکمیت اطلاعات حرکت می‌کنند (شکل۳).

- غیرمتمرکز: واحدهای مختلف در سازمان مستقلانه برای حاکمیت اطلاعات تلاش می‌کنند، ولی در صورت لزوم به‌طور موقت همکاری دارند.
- فدرالی: واحدهای مختلف در سازمان عمدتاً حاکمیت اطلاعات را مستقل پیش می‌برند، اما به‌صورت رسمی سازوکارهای ارتقای هم‌سویی بین آنها وجود دارد که معمولاً در قالب یک کمیته یا شورا ارائه می‌شود.
- متمرکز: یک واحد مستقل یا یک تیم تخصصی در یک واحد در درجهٔ اول مالک حاکمیت اطلاعات است، ولی شورای راهبری هم وجود دارد.

در مدل غیرمتمرکز تصمیم‌گیری به کسب‌وکار واگذار می‌شود، در مدل متمرکز تصمیم‌گیری در یک واحد بومی می‌شود، اما مدل فدرالی جنبه‌های راهبردی را متمرکز و جنبه‌های تاکتیکی را به کسب‌وکار می‌سپارد. در همهٔ مدل‌ها اهداف و بازیگران مشابه‌اند، اما این سردمداران امنیت و حفظ محرمانگی هستند که باید معایب و محاسن هر مدل در سازمان متبوع خود را بسنجند (شکل ۴) و مناسب‌ترین مدل را برگزینند.

چرا استقرار حاکمیت اطلاعات دشوار است؟

هرچند بر تعریفی یکتا از حاکمیت اطلاعات اتفاق نظر وجود ندارد، اما باید توجه داشت که هیچ‌یک از این تعاریف هیچ مفهومی از اجبار را نمی‌رسانند، بلکه حاکمیت را به مسئولیت‌پذیری مرتبط می‌کنند. وقتی با اطلاعات سروکار داریم همهٔ مشکلات از عدم‌مسئولیت‌پذیری ناشی می‌شود.

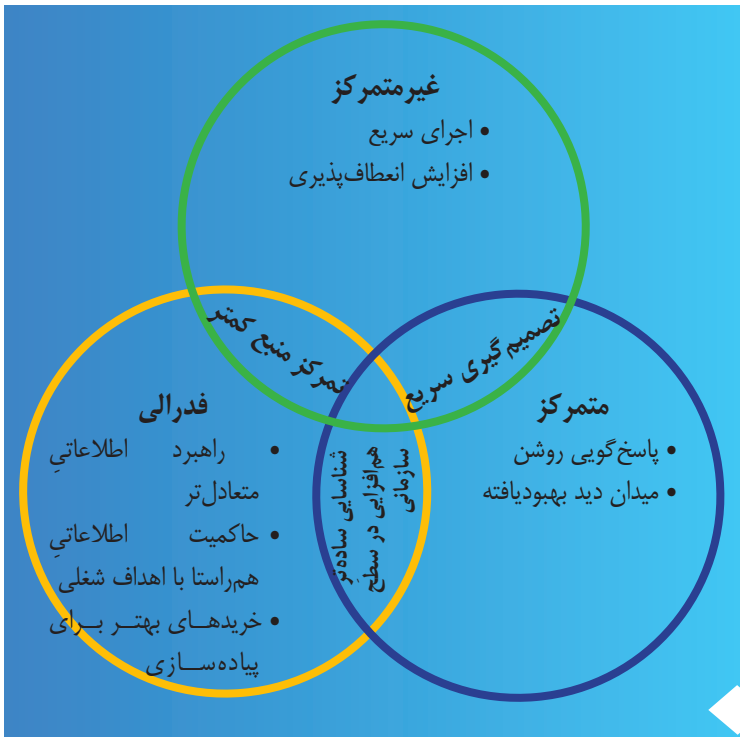
نه‌تنها حجم داده‌های سازمانی هر ۱۲ تا ۱۸ ماه دو برابر می‌شود، بلکه ممکن است داده‌ها در صدها محل ذخیره‌سازی در سراسر سازمان و یا در هر نقطه از جهان نگهداری شوند. کارمندان جابه‌جایی بسیاری دارند و از چندین دستگاه برای دسترسی به داده‌های موردنیاز خود استفاده می‌کنند و سازمان‌ها را مجبور می‌نمایند تا با فراهم کردن ارتباطات بهتر و برنامه‌های کاربردی روزآمدتر به انتظارات کاربران پاسخ دهند. انتظارات برای دسترسی در هر زمان، هر مکان و تقریباً از طریق هر دستگاهی چالش اطلاعات را همچنان دشوارتر می‌کند.

حاکمیت اطلاعات باید در سراسر سازمان گسترش یابد تا به نگرانی‌های مرتبط با رشد، خطرات، کارایی و هزینه‌ها رسیدگی شود. برنامه‌ریزی و مدیریت چنین چیزی چالش‌برانگیز خواهد بود.

نتیجه‌گیری

حاکمیت اطلاعات چهارچوبی است که ارکان آن افراد، فرایندها و فناوری هستند. تلاش برای گردآوری مواردی که ممکن است پیش از این عملکردی متفاوتی برای سازمان داشته بوده است، به‌منظور ایجاد رویکردی پایدار، قابل‌انطباق و مشارکتی برای مدیریت اطلاعات در برابر ریسک، زیر چتر حاکمیت اطلاعات قرار می‌گیرد. استقرار برنامهٔ حاکمیت اطلاعات از شرکتی به شرکت دیگر متفاوت است، اما هدف از آن باید یکسان باشد. حاکمیت اطلاعات پروژه‌ای با بازهٔ زمانی مشخص نیست بلکه برنامه‌ای نیازمند پشتیبانی مدیران اجرایی است. بیشتر سازمان‌ها برای اجرای برنامهٔ حاکمیت اطلاعات ازجمله ایجاد شورای حاکمیت مجبورند چندین بار مسیر را از ابتدا تکرار کنند. مهم این است که با درک این موضوع که هیچ «راه‌حل جادویی» یا فناوری خاصی برای ایجاد حاکمیت اطلاعات برای سازمان شما وجود ندارد این فرایند را آغاز کنید. به یاد داشته باشید حاکمیت اطلاعات یک چهارچوب است، ایستا نیست و باید بازتاب‌دهندهٔ الزامات فعلی و در حال ظهور برای مدیریت و استفاده از اطلاعات به‌عنوان دارایی سازمان باشد.

شکل ۳- سه مدل حاکمیت اطلاعات در سازمان‌ها



شکل ٤- منافع مدل‌های سه‌گانهٔ حاکمیت داده

پایداری در ضبط تصاویر سامانهٔ نظارت تصویری

نویسنده:
محمد قلم‌چی

یکی از ویژگی‌های مهم و ضروری سامانه‌های نظارت تصویری، امکان دسترسی همیشگی کاربر به تصاویر ضبط‌شده‌ی باکیفیت است. اطمینان از ضبط باکیفیت تصاویر از یک سو و توانایی ضبط طولانی تصاویر از سوی دیگر یک انتظار معمول از سامانه‌های نظارت تصویری است.

ضبط تصاویر در سامانه‌های نظارت تصویری به دلایل مختلف ممکن است به‌طور کلی با اختلال مواجه شود یا به‌درستی انجام نشود، مثلاً امکان دارد تصاویر ضبط‌شده با وجود کیفیت قابل‌قبول یا حتی بسیار خوبِ دوربین با کیفیتِ خوبی ضبط نشوند. در این مقاله در آغاز دلایل اختلال در ضبط تصاویر را بررسی می‌کنیم و سپس با تحلیل این دلایل و همچنین تحلیل هزینهٔ ناشی از هریک، روش‌های پیشگیری از آنها را برمی‌شمریم.

تعاریف

در سراسر این متن با عبارات و اصطلاحاتی مواجه خواهیم شد که ممکن است ناآشنا یا دارای چندین معنا باشند به همین سبب در آغاز، تعاریف موردنظر در این نوشته را ذکر می‌کنیم تا در ادامهٔ متن راهگشا باشند و به درک بهتر مطالب کمک کنند.

پایداری: مفهومی در علوم کامپیوتر است و به معنای توانایی کاربر برای دسترسی به اطلاعات یا منابع در یک مکان مشخص و در قالب صحیح است.

افزونگی[1]: به معنی قراردادن زیربخش‌های مشابه در یک سامانه به‌طور هم‌زمان و به‌صورت موازی است، به طوری که عملکرد کلی سامانه در شرایط اضطرار یا خطا تضمین شود و به بیان دیگر سطح پایداری سیستم افزایش یابد.

مرکز عملیات امنیت[2]: زیرساختی است برای استقرار تیم امنیت اطلاعات. این تیم مسئولیت نظارت بر سازمان و تحلیل وضعیت امنیتی آن را به‌صورت مداوم بر عهده دارد.

ذخیره‌ساز متصل به شبکه[3] (NAS): فضای ذخیره‌سازی متصل به شبکه یک سازوکار ذخیره‌سازی اطلاعات در قالب فایل (در مقایسه با ذخیره‌سازی در قالب بلاک) است که به یک شبکهٔ کامپیوتری متصل می‌شود و دسترسی داده‌ها به یک گروه ناهمگون از مشتریان را فراهم می‌کند. کارکرد ویژهٔ NAS نگهداری از فایل‌ها و در اختیار گذاردن آنها از طریق سخت‌افزار، نرم‌افزار و پیکربندی تخصصی بر بستر شبکهٔ کامپیوتری است.

شبکهٔ ذخیره‌سازی[4] (SAN): شبکه‌ای پرسرعت است که از تجهیزات ذخیره‌سازی اطلاعات تشکیل شده که آن تجهیزات نیز به‌نوبهٔ خود به سرورهای سخت‌افزاری یا مجازی متصل شده‌اند. ساختار ذخیره‌سازی اطلاعات در این نوع شبکه‌ها بلوکی است. به این خاطر نرم‌افزارهای کاربردی که روی سرورهای شبکه وجود دارند، به‌راحتی می‌توانند از طریق شبکه به اطلاعات موجود در SAN دسترسی پیدا

1- Redundancy
2- Security Operation Centre
3- Network Attached Storage
4- Storage Area Network

کنند. دستگاه‌های ذخیره‌سازی اطلاعات SAN می‌توانند شامل کتابخانهٔ نوارهای مغناطیسی هم باشند، اما در بیشتر موارد از هارد دیسک‌های سخت‌افزاری تشکیل شده‌اند که در کنار هم قرار گرفته‌اند و در قالب RAID در SAN کار می‌کنند.

دلایل عدم ضبط تصاویر

هر نوع اختلال در ضبط تصاویر تولیدشده توسط دوربین‌های نظارتی ممکن است باعث نقض یکی از وجوه سه‌گانهٔ امنیت شود. این رخداد در واقع نقض امنیت در یک سامانهٔ مراقبتی امنیتی است که شاخص‌های لازم برای اعتماد به اطلاعاتِ دریافت‌شده از آن را به‌شدت تحت تأثیر قرار می‌دهد و در هر سطحی غیرقابل‌قبول است. شناسایی عوامل بروز این اختلال‌ها به پیشگیری از وقوع آنها کمک می‌کند یا احتمال رخدادن آنها را به کمترین مقدار کاهش می‌دهد. در نمودار ۱، دلایل عدم ضبط تصاویر دسته‌بندی شده‌اند.

برخی از دلایل باعث عدم ضبط باکیفیت لحظه‌ای تصاویر و برخی موجب از دست رفتن کامل ضبط تصاویر می‌شوند. البته برخی دلایل عدم ضبط باکیفیتِ لحظه‌ای نیز ممکن است موجب عدم ذخیره‌سازی بلندمدت شوند.

اختلال لحظه‌ای

میزان بالای تحرک اجزای صحنه یا نویز در ویدئو

وقتی میزان تحرک اجزای موجود در صحنه زیاد می‌شود، اندازهٔ حجم فریم‌های تصویر به‌میزان قابل‌توجهی افزایش می‌یابد. افزایش حجم نویز (که بیشتر در شب و به‌دلیل استفاده از قابلیت‌هایی همچون کنترل بهره در لحظه رخ می‌دهند) نیز تأثیر مشابهی دارد. در برخی از این لحظات، ممکن است دوربین توانایی فشرده‌سازیِ لحظه‌ایِ تصاویر را نداشته باشد و یا ذخیره‌ساز نتواند تصویر حجیم را ذخیره کند.

قطع‌شدن برق

هر دستگاه الکترونیکی با قطع جریان الکتریکی یا از کار افتادن منبع تولید توان مصرفی آن، اعم از باطری یا سلول خورشیدی یا برق شهری، از کار می‌افتد.

دریافت دادهٔ نادرست (نفوذ و ...)

روش‌های متعددی برای نفوذ به سامانهٔ نظارت تصویری وجود دارد. اگر مهاجمی بتواند به‌گونه‌ای به سامانه نفوذ کند

ممکن است تصاویر جعلی برای ذخیره‌ساز ارسال نماید یا ارتباط دادهای میان دوربین مداربسته و ذخیره‌ساز را از بین ببرد.

حملات محروم‌سازی توزیع‌شده از سرویس[5] (DDOS)

حملات سایبری متعددی برای از کار انداختن سامانهٔ نظارت تصویری انجام می‌شود. مهم‌ترین آنها DDos، حملات محروم‌سازی توزیع شده از سرویس یا انکار سرویس است. اگر مهاجمی به‌طور متناوب دوربین مداربسته یا دستگاه ذخیره‌ساز را با ارسال درخواست‌های دسترسی مکرر به خود مشغول کند، ممکن است موجب از کار افتادن منبع تصویر یا دستگاه ذخیره‌ساز شود.

قطع ارتباط دادهٔ میان دوربین مداربسته و ذخیره‌ساز

مشکلات شبکه، یکی از مسائل شایع در سامانه‌های نظارت تصویری تحت شبکه است. در سامانه‌های نظارت تصویری آنالوگ نیز ضعف بستر ارتباطی، غالباً باعث بروز میزان قابل‌توجهی از ضعف یا از دست رفتن ارتباط میان دوربین مداربسته و ذخیره‌ساز است.

عمل‌نکردن لحظه‌ای ذخیره‌ساز به‌دلیل بالارفتن دما

متأسفانه در بسیاری از پروژه‌ها، به کنترل دمای ذخیره‌سازِ سامانهٔ نظارت تصویری در محدودهٔ مجاز عملکردی آن که در دفترچهٔ راهنما یا جدول مشخصات آن درج شده است، توجه کافی نمی‌شود. دستگاه ذخیره‌ساز مانند هر دستگاه الکترونیکی دیگر با افزایش دمای محیط ممکن است به‌دلیل تحمل دمای بیشتر از محدودهٔ مجاز، به صورت موقتی یا دائم از کار بیفتد.

پهنای باند نازل دستگاه ذخیره‌ساز

تجهیزات ذخیره‌ساز، خصوصاً تجهیزات خوداتکا[6] همچون NVR، DVR و XVR پهنای باند محدودی برای ارتباط با دوربین‌ها دارند. اگر از دوربین‌هایی با کیفیت بالا استفاده شود، این کمبود پهنای باند هرچه بیشتر به چشم می‌آید. گاهی در پروژه‌ها به‌منظور دستیابی به امکان ذخیره‌سازی تصویر تمامی دوربین‌ها، کیفیت تصویر دوربین‌ها کاهش پیدا می‌کند. همچنین با بالارفتن پهنای باند مصرفی لحظه‌ای تمام یا برخی از دوربین‌ها، این محدودیت پهنای باند ممکن است موجب اختلال در ضبط تمام تصاویر یا برخی از آنها شود.

اختلال بلندمدت

به سرقت رفتن یا از بین رفتن فیزیکی ذخیره‌ساز یا هارد دیسک‌ها

با افزایش سطح اطلاع، دانش و تخصص مهاجمان، سارقان و شورشیان، اولین اقدام ایشان در زمان ورود به مکانی که دارای سامانهٔ نظارت تصویری است، سرقت یا از بین بردن دستگاه یا سرور ضبط تصاویر یا حداقل هارد دیسک‌های آن است.

سوختن هارد دیسک به دلیل مدیریت ناصحیح داده در ذخیره‌ساز

برای بیشتر تجهیزات مستقل نظارت تصویری این مشکل به‌وجود می‌آید که هارد دیسکشان بسوزد. حجم بالای ترافیک داده که بدون هیچ مدیریتی برای ذخیره‌سازی به‌سوی هارد دیسک سرازیر می‌شود دمای آن را افزایش می‌دهد و موجب سوختن آن می‌شود.

سوختن یا عمل‌نکردن طولانی ذخیره‌ساز

به دلایل مختلف، از جمله پایان طول عمر ذخیره‌ساز، ممکن است ذخیره‌ساز از کار بیفتد. اگر بهره‌بردار به‌موقع از خطرِ سوختن ذخیره‌ساز آگاه شود، آن را جایگزین خواهد نمود، اما اگر صحنه‌ای مهم به دلیل عدم‌تصویربرداری دستگاهِ ازکارافتاده از قلم بیفتد، قابل‌جبران نخواهد بود.

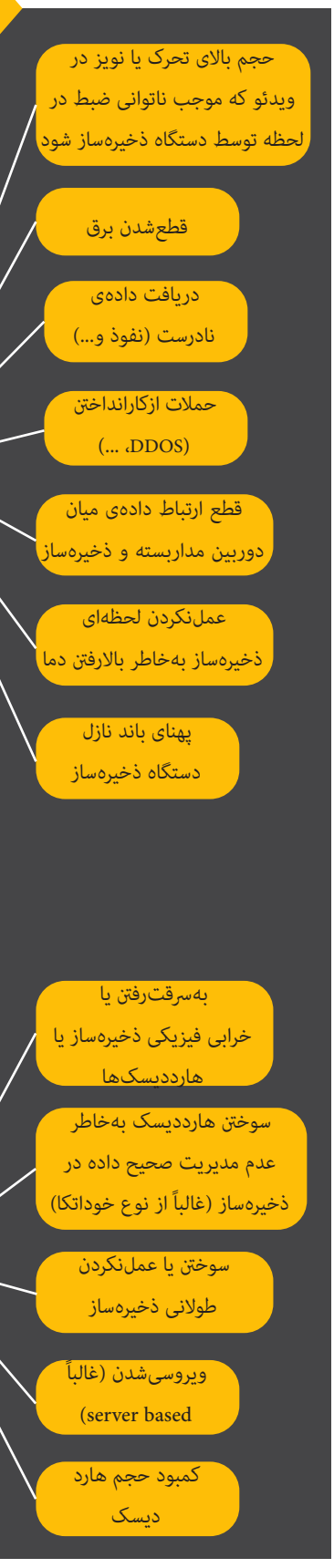
ویروسی‌شدن

در صورتی که سامانهٔ مستقل نظارت تصویری یا سرور ذخیره‌سازیِ تصاویر ویروسی شود. این ویروس‌ها ممکن است باعث پاک‌شدن فایل‌ها شوند. همچنین ممکن است سرور ذخیره‌سازِ تصاویر، هدف باج‌گیری داده قرار بگیرد.

کمبود حجم هارد دیسک

بسیاری از مواقع نیازمند دسترسی به تصاویری هستیم که

نمودار ۱- بررسی دلایل



5- Distributed Denial of Service
6- Standalone

به‌دلیل کمبود حجم ذخیره‌سازی در گذشته پاک شده‌اند.

روش‌های افزایش سطح پایداری ضبط تصاویر

برای بهبود شاخص‌های ضروری امنیت در سامانهٔ نظارت تصویری لازم است تا پس از شناخت عوامل مؤثر در ایجاد اختلال در ضبط یا انتقال تصاویر بر اقداماتی متمرکز شویم که به‌طور کلی پایدارسازی عملکرد سامانه و به‌طور خاص، پایداری فرایند ضبط و انتقال تصاویر را در پی دارند. پایدارسازی عملکرد ضبط در سامانهٔ نظارت تصویری، از شیوه‌هایی که به‌صورت جامع در نمودار ۲ دسته‌بندی شده‌اند قابل‌دستیابی است. شرح هریک از بلوک‌های این نمودار در ادامه آمده است.

پایداری منبع تصویر

واضح است که شرط لازم ضبط درست تصاویر در ابتدا، وجود محتوای موردنظر یا به بیان دیگر «پایداری منبع تولید تصویر» است. مهم‌ترین اقداماتی که برای افزایش سطح پایداری منبع تولید تصویر باید صورت بگیرند در ادامه آمده‌اند.

افزایش امنیت فاوا

یکی از مواردی که منبع تصویر را ضایع خواهد کرد، اختلال‌هایی است که بر اثر حملات سایبری ممکن است رخ دهد. برای جلوگیری از این تهدیدها، راهکارهای زیر مفید هستند:

- کنترل سطح امنیتی دوربین قبل از تأمین: بررسی سطح امنیت، پایداری و اصالت تجهیزات نظارت تصویری با تکیه بر گزارش آزمایشگاه‌هایی که برای این منظور وجود دارند. همچنین انجام آزمایش‌های امنیتی توسط تیم‌های متخصص، از تأمین تجهیزاتی که مستعد تهدیدهای متعددی هستند، جلوگیری می‌کنند.
- پیاده‌سازی مرکز عملیات تخصصی امنیت نظارت تصویری: دوربین‌های مداربستهٔ تحت شبکه به‌طور کامل در بستر شبکه کار می‌کنند. سامانه‌های نظارت تصویری آنالوگ نیز از ذخیره‌سازهایی استفاده می‌کنند که درگاه شبکه دارند، بنابراین پیشنهاد می‌شود این تجهیزات نیز جزو تجهیزات موردبررسی در مرکز امنیت الکترونیکی قرار بگیرند.

افزونگی منبع تصویر

افزونگی می‌تواند در سه سطح منابع تغذیه، شبکهٔ انتقال داده و دوربین مداربسته پیاده‌سازی شود که در ادامه توضیح مختصری دربارهٔ هریک از آنها ارائه می‌شود.

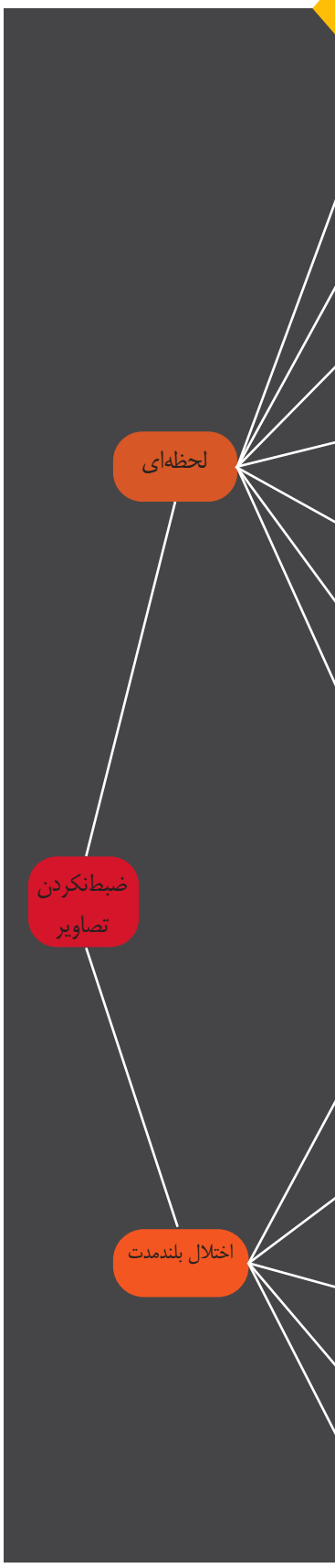
- افزونگی منابع تغذیه: تأمین برق از بیش از یک روش یا منبع تغذیه به‌همراه قابلیت جایگزینی منبعِ دچار مشکل با منبع جدید موجب می‌شود تا عملکرد دوربین مداربسته یا ذخیره‌ساز، به‌دلیل قطعی برق دچار اختلال نشود. این افزونگی می‌تواند در سطوح متفاوتی پیاده‌سازی شود. مثلاً می‌توان برای دوربین مداربسته، برق مصرفی را هم از طریق آداپتور و هم از طریق PoE[7] (با قابلیت سوئیچ بین این دو) تأمین کرد یا در دستگاه ذخیره‌ساز، از دو منبع تغذیهٔ موازی با قابلیت جایگزینیِ خودکار بهره برد.
- افزونگی شبکهٔ انتقال داده: پیاده‌سازی بیش از یک شبکهٔ انتقال داده موجب می‌شود تا در صورت قطع‌شدن یک شبکه، بتوان با بهره‌برداری از سوئیچ محلی، به شبکهٔ دیگر انتقال یافت. اما به‌دلیل امکان بروز مشکلات متعدد از جمله خرابی سوئیچ محلی و افزایش مخاطرات امنیتی این راهکار توجیه اقتصادی و فنی قابل‌قبولی ندارد.
- افزونگی دوربین مداربسته: با نصب بیش از یک دوربین در یک موقعیت (با همان زاویهٔ دید)، افزونگی دوربین محقق می‌شود ولی به‌دلیل بار مضاعف روی شبکه، هزینهٔ بالا و همچنین امکان از کار افتادن دوربین دوم، به‌خاطر مشکلاتی که برای دوربین اول پیش آمده، به‌ندرت از این راهکار استفاده می‌شود و دارای توجیه فنی و اقتصادی قابل‌قبولی نیست.

پایش برخط با سامانهٔ مدیریت سلامت نظارت تصویری

پایش مستمر و در لحظهٔ سامانهٔ نظارت تصویری امکان نظارت بر درستی کارکرد دوربین و ذخیره‌ساز را فراهم می‌کند تا در صورت بروز خطا در عملکرد هریک، بهره‌بردار بی‌درنگ آگاه شود و اقدامات لازم به‌منظور رفع ایرادها را اجرا کند. به همین دلیل استقرار و بهره‌برداری از این سامانه اهمیت ویژه‌ای دارد.

پایداری ذخیره‌ساز

روش‌های افزونگی پیشرفته و مبتنی بر فناوری



7- Power of Ethernet

اطلاعات

افزونگی در ضبط، یکی از مؤثرترین راه‌ها برای اطمینان از پایداری همیشگی عملیات ضبط است. راهکارهای نوین و تجهیزات تخصصی ذخیره‌سازی در فناوری اطلاعات، معتبرین‌ترین شیوهٔ تخصصی ایجاد افزونگی در ضبط هستند که این افزونگی به یکی از روش‌های زیر قابل‌پیاده‌سازی است.

- بهره‌برداری از FTP[8] دستگاه ضبط و مدیریت تصاویر: در تنظیمات برخی دستگاه‌های مستقل، همچون NVR/DVR، امکان معرفی سروری برای ارسال فایل‌های ذخیره‌شده وجود دارد، اما تجربه نشان داده این اقدام در بیشتر تجهیزات موجود به‌درستی محقق نمی‌شود و قابل‌اتکا نیست. پیاده‌سازی سرور انتقال فایل برای ضبط فایل‌های تصویری نیازمند سرورهایی است که از سرعت بالایی برخوردارند و می‌توانند فایل‌های حجیم را مدیریت کنند و لزوماً گران‌قیمت هم نیستند.

8- File Transfer Protocol

- بهره‌برداری از FTP نرم‌افزار سامانهٔ مدیریت تصاویر[9] (VMS): برخی نرم‌افزارهای موسوم به سامانهٔ مدیریت تصاویر، قابلیت دارند به‌طور خودکار فایل‌های ضبط‌شده را به سرورهای FTP ارسال کنند. البته باید یادآور شویم که پیاده‌سازی چنین سروری با قابلیت مدیریت فایل‌های حجیم، نیازمند تأمین FTP پرسرعت، ویژهٔ نظارت تصویری، است که قیمت بالایی دارد.
- پیاده‌سازی سرور کپی‌برداری هوشمند: در سامانه‌های مدیریت تصویر با قابلیت مدیریت فایل، امکان پیاده‌سازی سرور مدیریت هوشمندِ انتقال فایل وجود دارد. بدین ترتیب به‌صورت مرکزی برای سازمان‌ها، ذخیره‌ساز محلی ایجاد می‌شود.
- بهره‌برداری از استریم مستقیم دوربین‌های مداربسته: ضبط مستقیم استریم دریافتی از دوربین مداربسته برای دوربین‌های تحت شبکه و انکودر یا DVR برای دوربین‌های آنالوگ یا HDoC مطمئن‌ترین شیوهٔ افزونگی است. زیرا دستگاه ذخیره‌ساز دوم به دستگاه ذخیره‌ساز اول وابسته نیست. تنها نگرانی در این راهکار، ایجاد ضعف در استریم دوم دریافتی است که در دوربین‌های تحت شبکه که در ردهٔ سازمانی هستند، مشکلی ایجاد نخواهد کرد. دستگاه‌های خوداتکای ضبط با کمینهٔ کیفیت نیز، توانایی ارائهٔ دست‌کم یک استریم اضافی دارند و مشکلی در این رابطه برای آنها به‌وجود نمی‌آید. بهتر است قبل از به کار گرفتن این راهکار، توانایی تجهیزات خود را عملاً بررسی کنید.

9- Video Management System

* ضبط مستقیم استریم با نرم‌افزار سامانهٔ مدیریت تصاویر: برخی نرم‌افزارهای توانمند سامانهٔ مدیریتِ تصاویر می‌توانند انواع استریم تصویر را از منابع تصویری مختلف نظیر دوربین مداربستهٔ تحت شبکه و DVR دریافت کرده و ذخیره‌سازی نمایند. برخی از این نرم‌افزارهای نظارت تصویری توانایی فشرده‌سازی مجدد این تصاویر را نیز دارند.
* ضبط مستقیم استریم با ذخیره‌ساز متصل به شبکه: ذخیره‌ساز متصل به شبکه، قابلیت دریافت مستقیم استریم ویدئویی و ذخیره‌سازی آن را دارد. این دستگاه ذخیره‌سازی گران‌قیمت است و به همین دلیل غالباً استفاده از آن در حوزهٔ نظارت تصویری توجیه اقتصادی ندارد.
* مضاعف‌سازی دستگاه ذخیره‌ساز
  - استفادهٔ مضاعف دو دستگاه مستقل: در خصوص دستگاه NVR، می‌توان یک دوربین مداربسته را در دو NVR مختلف تعریف کرد. در

ماتریس تأثیرگذاری

دلایل ازبین‌رفتن پایداری
حجم بالای تحرک یا نویز در ویدئو که موجب ناتوانی ضبط دستگاه ذخیره‌ساز شود
قطع‌شدن برق
دریافت دادهٔ نادرست (نفوذ و ...)
حملات از کار انداختن (DDOS، ...)
قطع ارتباط دادهٔ میان دوربین مداربسته و ذخیره‌ساز
عمل‌نکردن لحظه‌ای ذخیره‌ساز به‌دلیل بالارفتن دما
پهنای باند نازل دستگاه ذخیره‌ساز
به سرقت رفتن یا از بین رفتن فیزیکی ذخیره‌ساز یا هارد دیسک‌ها
سوختن هارد دیسک به‌دلیل مدیریت ناصحیح داده در ذخیره‌س (Alone
سوختن یا عمل‌نکردن طولانی ذخیره‌ساز
ویروسی‌شدن (غالباً Server based)
کمبود حجم هارد دیسک
تعداد کل تهدیدهای پوشش‌داده‌شده

این صورت اگر یکی از کار بیفتد، دیگری ذخیره‌سازی را انجام می‌دهد. در خصوص DVR به‌دلیل لزوم اتصال مستقیم به دوربین مداربسته، باید از یک DVR به DVR دیگر ورودی داد یا با استفاده از فیش‌های کپی‌بردار، نظیر فیش T، یک دوربین را به دو DVR متصل نمود.

- استفادهٔ هم‌زمان از یک دستگاه خوداتکا و VMS: چه NVR داشته باشیم و چه DVR، برخی VMSهای مدرن، همچون امن‌پایش، قابلیت دریافت استریم ویدئو را به‌صورت مستقیم از دوربین تحت شبکه یا DVR دارند و می‌توانند به‌عنوان ذخیره‌ساز پشتیبان استفاده شوند.

روش‌های افزایش پایداری	کنترل آزمایشگاهی عملکرد دوربین قبل از تأمین	پیاده‌سازی SOC تخصصی نظارت تصویری	افزونگی منابع تغذیه	افزونگی شبکهٔ انتقال داده	افزونگی دوربین مداربسته	پایش برخط با سامانهٔ مدیریت سلامت نظارت تصویری	بهره‌برداری از NVR/DVR دستگاه FTP	بهره‌برداری از FTP نرم‌افزار VMS	پیاده‌سازی سرور کپی‌برداری هوشمند (ویژهٔ VMS)	ضبط مستقیم استریم با نرم‌افزار VMS	ضبط مستقیم استریم با NAS	غلبه بر خرابی	ضبط در لبه
ط درلحظه توسط	✓	–	–	–	–	–	–	–	–	✓	✓	–	–
	–	–	✓	–	–	–	–	–	–	–	–	–	–
	✓	✓	–	–	–	–	–	–	–	–	–	–	–
	✓	✓	–	–	–	–	–	–	–	–	–	–	–
	–	–	–	✓	✓	✓	–	–	–	✓	✓	–	–
	–	–	–	–	–	✓	–	–	–	✓	✓	✓	✓
	✓	–	–	–	–	–	–	–	–	✓	✓	–	–
	–	–	–	–	–	✓	–	✓	✓	✓	✓	–	–
ساز (غالباً Stand	–	–	–	–	–	✓	–	–	✓	✓	✓	–	–
	–	–	–	–	–	✓	–	–	–	✓	✓	✓	–
	–	✓	–	–	–	✓	–	–	✓	✓	✓	–	–
	–	–	–	–	–	✓	–	–	✓	✓	✓	–	–
	۴	۳	۱	۱	۱	۷		۱	۴	۹	۹	۲	۱

پایش برخط با سامانهٔ مدیریت سلامت نظارت تصویری

پایش برخط صحت عملکرد منابع تصویری و ذخیره‌سازی آنها، کارکرد اصلی سامانهٔ مدیریت سلامت نظارت تصویری است.

روش‌های معمول سامانه‌های نظارت تصویری

در سامانه‌های نظارت تصویری، عموماً از روش‌های مشخصی برای بهبود سطح پایداری استفاده می‌شود. نکتهٔ مهم آن است که این ویژگی‌ها غالباً از ویژگی‌های توکار تجهیزات نظارت تصویری است و امکان ارتقای آن برای سامانهٔ موجود عموماً وجود ندارد. از سوی دیگر، اکثر این روش‌ها صرفاً در سامانه‌های نظارت تصویری مبتنی بر دوربین‌های تحت شبکه کاربرد دارند.

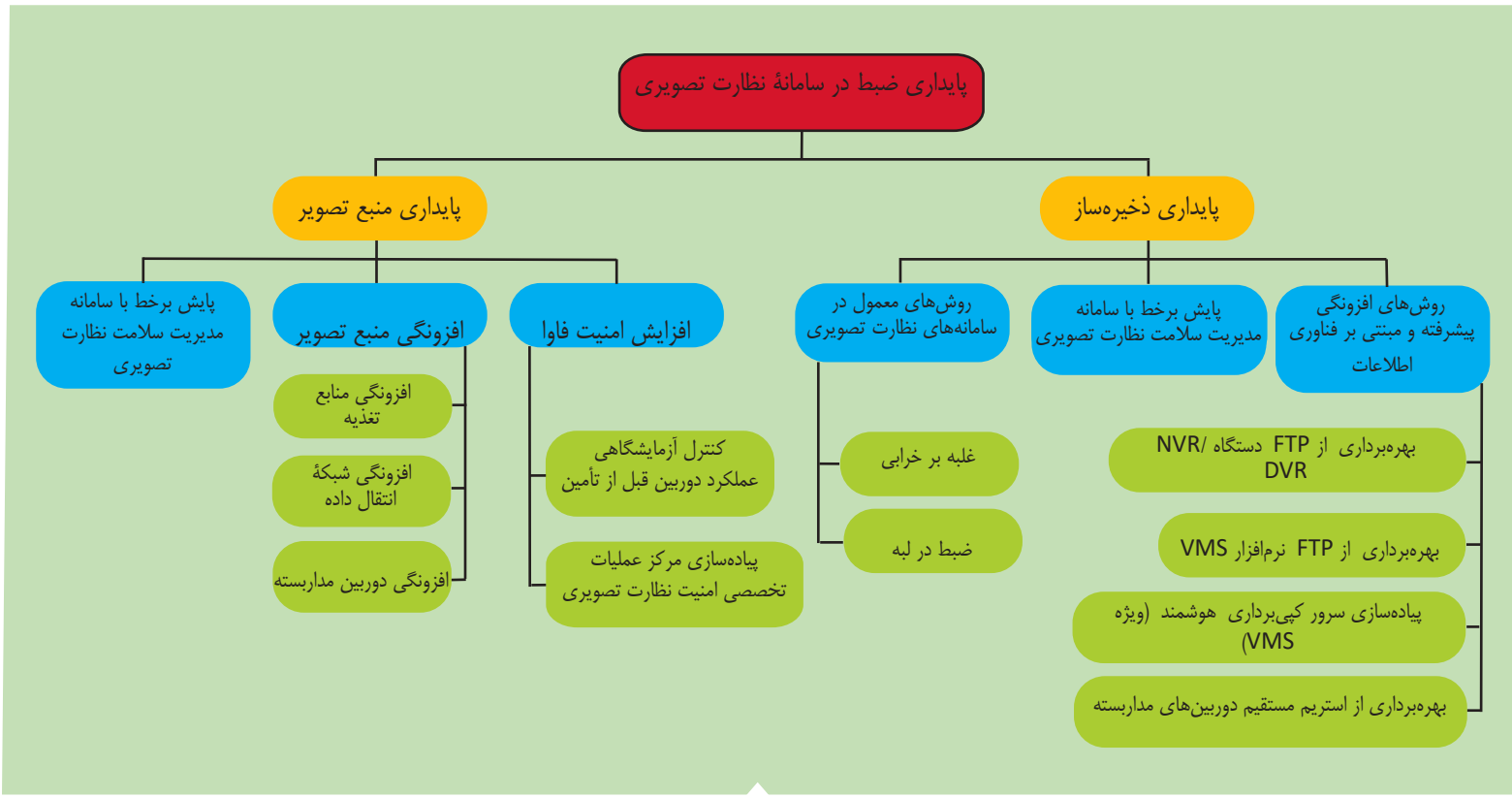
– «غلبه بر خرابی»[10]: در علوم کامپیوتر و علوم مرتبط همچون شبکه و نظارت تصویری، این واژه به معنی جابه‌جایی از یک تجهیز یا سرویس به یک تجهیز یا سرویس کاملاً مشابه است که به‌صورت افزونه تعبیه شده است، تا زمانی که خطا یا عملکرد غیرعادی پایان یابد. دستگاه یا سرویسی که در فرایند غلبه بر خرابی عملیات به آن محول شده است، عملکردی مشابه دستگاه یا سرویس اولیه دارد و این فرایند به‌صورت نامحسوس و کاملاً خودکار صورت می‌گیرد.

در برخی محصولات، می‌توان تعدادی NVR را به‌صورت پشتیبانِ غلبه بر خرابی تنظیم نمود، یعنی وقتی یکی از دستگاه‌ها به هر دلیل از کار افتاد، دستگاه NVR دیگر، که به صورت آماده‌به‌خدمت، منتظر جایگزینی است و منابعی به آن اختصاص نیافته است، به‌صورت خودکار ضبط تصاویر دوربین‌هایی را که به دستگاه قبلی متصل بودند به‌عهده می‌گیرد. به دلیل اتصال فیزیکی دوربین‌های آنالوگ به DVR، پیاده‌سازی آرایش غلبه بر خرابی در دوربین‌های آنالوگ تقریباً ممکن نیست.

– «ضبط در لبه»[11]: برخی دوربین‌های مداربستهٔ تحت شبکه می‌توانند تصاویر را

10- Failover

11- On edge recording



نمودار ۲- درخت دسته‌بندی راهکارهای افزایش پایداری در ضبط نظارت تصویری

روی کارت‌های حافظه‌ای که روی خودِ دوربین نصب شده، ذخیره کنند. اگر NVR یا نرم‌افزار سامانهٔ مدیریت تصاویر امکان انتقال تصاویر ضبط‌شده به کارت حافظهٔ نصب‌شده روی دوربین را، در مواقعی که تصویر به هر دلیل قطع شده، داشته باشد، ضبط در لبه انجام داده است. این قابلیت نیز مختص دوربین‌های مداربستهٔ تحت شبکه است. البته این قابلیت چندان قابل‌اتکا نبوده و سوابقی از عملکرد نادرست آن دیده شده است.

ماتریس تأثیرگذاری

تا اینجا تلاش شد تا تمامی عوامل مؤثر در اختلال در ضبط تصاویر در سامانه‌های نظارت تصویری و راهکارهای مقابله یا گذر از آنها بررسی شوند. برای تکمیل بحث و همچنین سهولت کاربرد، در قالب ماتریس میزان تأثیرگذاری عوامل مختلف بر عدم ضبط تصاویر و میزان تأثیرگذاری روش‌های افزایش پایداری ضبط آورده شده است.

نتیجه‌گیری

انتخاب راهکار بهینه برای افزایش پایداری ضبط در سامانهٔ نظارت تصویری

با دقت در نتایج تحلیل مندرج در ماتریس تأثیرگذاری و توضیحات تکمیلی ارائه‌شده، اقدامات لازم برای اطمینان از پایداری تصاویر در سامانهٔ نظارت تصویری یک سازمان را می‌توان در بندهای زیر خلاصه کرد:

پیاده‌سازی سامانه مدیریت سلامت نظارت تصویری

این سامانه عملکرد دقیق سامانهٔ نظارت تصویری را به‌صورت برخط پایش می‌کند و اگر مشکلی در منابع تصویری (دوربین‌های مداربسته)، شبکهٔ انتقال داده یا ذخیره‌ساز رخ دهد، اطلاع‌رسانی می‌کند. همچنین تا حد زیادی دلیل بروز مشکل را مشخص خواهد کرد و موجب می‌شود در آینده از بروز مجدد آن جلوگیری شود.

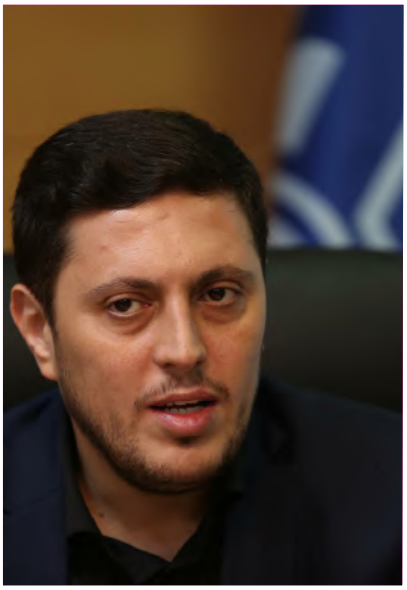
بهره‌برداری از استریم مستقیم دوربین‌های مداربسته برای ذخیره‌سازی افزونه

اگر ذخیره‌سازی مضاعف محلی موردنظر باشد، با در نظر گرفتن زمان موردنیاز برای ذخیره‌سازی مضاعف، ضبط مستقیم استریم با نرم‌افزار سامانهٔ مدیریت تصاویر پیشنهاد می‌شود. اگر هم ذخیره‌سازی مرکزی، با معماری گسترده در کشور با فرض ارتباط شبکهٔ اختصاصی با پهنای باند محدود، مدنظر باشد و از سامانهٔ مدیریت تصاویر نیز بهره گرفته شده باشد، پیاده‌سازی سرور کپی‌برداری هوشمند، ویژهٔ سامانهٔ مدیریت تصاویر، راهکار مناسبی خواهد بود.

نشست با یاسر باقری مدیرکل بررسی‌های اقتصادی و توسعهٔ کسب‌وکار شرکت مخابرات ایران

«داده، کلیدی‌ترین عنصر انقلاب صنعتی چهارم»

مصاحبه‌کننده:
سیده مژگان سیدنقوی



یاسر باقری دانش‌آموخته‌ی مهندسی الکترونیک از دانشگاه خواجه نصیر و دانشجوی دکترای بازرگانی در دانشگاه تهران است. ۲۰ سال در حوزه‌های مختلف فناوری اطلاعات و ارتباطات فعالیت داشته و ۲ سال است که به خدمت در شرکت مخابرات ایران در حوزه‌ی بررسی‌های اقتصادی و توسعه‌ی کسب‌وکار مشغول شده است.

«همگرایی داده‌ها در ایران، نیاز اولیه برای اکوسیستم فناوری کشور»

نمایشگاه ایپاس ۱۴۰۲
غرفهٔ مخابرات
بخش مربوط به سرویس هوبان

دکتر یاسر باقری در نشست با سرویس مصاحبهٔ ویژهٔ نشریهٔ امنیت الکترونیک در خصوص حاکمیت داده[1] این‌چنین گفت:

«می‌خواهم از منظر دیگری به این موضوع نگاه کنم. واقعیت این است که ما در حالی از حاکمیت داده صحبت می‌کنیم که صنعتمان هنوز نتوانسته راه خودش را در بحث مدیریت داده پیدا کند. اگر گامی به‌عقب برگردیم و دقیق‌تر به این موضوع نگاه کنیم، می‌بینیم که لازم است هر سازمان و شرکت برای خودش راهبرد داده[2] تعریف کند و در ادامه و در ذیل آن به مدیریت داده[3] و حاکمیت داده بپردازد.

زمانی می‌توانیم این دو ماژول را به‌دقت پیگیری کنیم که راهبرد مشخصی راجع به داده داشته باشیم، به عبارت دیگر بر مبنای اسناد بالادستی بتوانیم دقیق‌تر، مشخص‌تر و عینی‌تر راجع به راهبرد داده صحبت کنیم و بعد از آن در حوزهٔ اجرا حرف از مدیریت داده بزنیم و اگر سامانه‌ها و ابزارهای داده‌ای [که در اختیار داریم] بتوانند نیازمندی‌های ما را برای اهداف تجاری و IT در سازمان ساپورت کنند [آن وقت] می‌توانیم کمی با حاکمیت داده درگیر شویم. ما در حاکمیت داده بیشتر از دیسیپلین و قوانین از کنترل داده صحبت می‌کنیم، در حالی که در سازمان‌ها، به‌عنوان مثال شرکت‌های بزرگی مثل شرکت مخابرات ایران، با توجه به پیچیدگی کار و تعداد زیاد مشتریان مسائلی در حوزهٔ حاکمیت داده وجود دارد که در فاز اول باید بتوانیم این موارد را راحت‌تر حل کنیم، در آن نقطه است که می‌توان دربارهٔ حاکمیت داده صحبت کرد. فکر می‌کنم خیلی از شرکت‌ها و سازمان‌هایی که در ایران کار می‌کنند در این قسمت مشکل دارند: اول اینکه نمی‌دانند چه راهبردی در حوزهٔ داده باید اتخاذ کنند و دوم با روندهای تحولات صنعت آشنا نیستند.

ما انقلاب صنعتی چهارم را داریم که در آن عملاً داده نقش دقیق و حیاتی دارد چه در بحث خط تولید، چه در اتوماسیون تولید و چه در حوزه‌های رباتیک. عملاً در همهٔ این موارد وقتی نگاه کارشناسی داشته باشیم، در می‌یابیم که کشور ما نتوانسته نمرهٔ خوبی در این حوزه کسب نماید. اگر بخواهیم در این مورد مبسوط صحبت کنیم باید گفت که در انقلاب صنعتی چهارم از IoT[4] و INDUSTRIAL CYBER PHISICAL SYSTEM[5] صحبت می‌کنیم و حوزهٔ گسترده‌ای راجع

1- Data governance
2- Data strategy
3- Data management

۴- اینترنت اشیا
۵- سامانهٔ سایبری فیزیکی صنعتی

به سنسورها داریم. همهٔ اینها این نیاز را ایجاد می‌کنند که یک جریان دادهٔ مدون و مطمئن و کنترل‌شده با دیسیپلینی خاص و هم‌راستا با اهداف تجاری پیاده‌سازی شود. در این مقطع است که بحث حاکمیت داده جدی می‌شود.

فکر می‌کنم اگر بخواهیم دوباره از انقلاب‌های صنعتی عقب نیفتیم، واقعاً چاره‌ای نداریم که در بحث مدیریت داده و حاکمیت داده که دو ماژول جداگانه در ذیل راهبرد داده هستند، تکلیف خودمان را مشخص کنیم، چه در حوزهٔ آکادمیک و چه در حوزهٔتجربی و به‌خصوص [در رابطه با] واحدهای تولید داده در صنعت. در تمام این موارد نیازمند هم‌گرایی هستیم تا در اولین گام بتوانیم با تشخیص

«داده‌هـــای مـلی، سرمایـه‌هـای ارزشمند کشور هستند»

وضعیت موجود نقشهٔ راه داده در کشور را به‌درستی تدوین کنیم. به‌نظر می‌رسد دولت در این بین نباید خیلی دنبال نقش‌آفرینی واحدی باشد؛ چراکه در دنیا ثابت شده است که بیشتر اوقات خود اکوسیستم و خود بازار مسیر درست رشد و تعالی را پیدا می‌کند. وقتی حرف از داده می‌زنیم، یکی از موضوعات بسیار مهم حاکمیت است. در حوزهٔ حاکمیت راجع به کیفیت داده[6] صحبت می‌کنیم تا مطمئن شویم که از این داده‌ها در راستای بیزینس ما استفاده می‌شود یا خیر؟ ولی چرا ما این ضرورت را جدی نمی‌گیریم؟ شاید به‌دنبال ایجاد جنگلی از سامانه‌ها هستیم، به‌جای اینکه به داده به‌عنوان دارایی[7] نگاه کنیم. اما امروز در بحث انقلاب صنعتی چهارم سازمان‌ها را به دو قسمت تقسیم می‌کنند: آنهایی که داده‌محور[8] هستند مثل

6- Data quality
7- Asset
8- Data-driven

«شرکت مخابرات ایران جزو ۱۰ شرکت برتر مخابراتی جهان»

شرکت‌هایی که در حوزهٔ فضای ابری کار می‌کنند و سازمان‌هایی که استفاده از داده در آنها فعال است[9] مثل بسیاری از بخش‌های صنعتی که از داده استفاده می‌کنند. [برای اینکه به‌سوی حاکمیت داده حرکت کنیم] لازم است رویکردمان به داده دارایی‌محور باشد و بر اساس همین رویکرد نیز برنامه‌ریزی کنیم.

شاید این موضوع هنوز برای کشور خیلی ضروری به‌نظر نرسد که دلیل آن هم احتمالاً نبود مدیریت و نگهداری بخش زیادی از داده‌های کلیدی است که به‌دلیل استفادهٔ عمومی از پلتفرم‌های غیربومی در اختیار کشور نیست، فلذا ما روی بخش وسیعی از این داده‌ها تسلط کافی نداریم و نمی‌توانیم از آنها برای تولید ثروت و ارزش افزوده استفاده کنیم در حالی که این موضوع سال‌هاست در دنیا اثبات‌شده و شرکت‌های فناوری داده‌محور را به شرکت‌های قدرتمندتری تبدیل کرده است. تحقیقات زیادی به‌منظور بررسی چالش‌های مرتبط با حاکمیت داده در کشور صورت گرفته است، اما به نظر من اولین چالش این است که [چرخهٔ] داده در کشورمان آزاد نیست. شرکت مخابرات ایران داده‌های خودش را دارد، سازمان‌ها و ارگان‌های دیگر نیز داده‌های خودشان را دارند و این جزیره‌های متعدد، داده را در کشور به‌بند کشیده است. عملاً فضایی نیست که با کنار هم گذاشتن این داده‌ها ارزش افزودهٔ بیشتری ایجاد شود و چون ارزش افزوده ایجاد نمی‌شود، عملاً [در] فضای اقتصادی و تجاری ضرورتی برای همکاری بین‌سازمانی به‌وجود نمی‌آید تا جریان ارتباط و اتصال داده‌ها در کشور آزاد شود. نکتهٔ ظریفی که در اینجا به‌چشم می‌خورد این است که فراتر از آنچه بیان شد در درون برخی سازمان‌ها نیز داده‌ها به‌صورت جزیره‌ای نگهداری می‌شوند و ارتباطی بین اجزای دادهٔ یک سازمان با مدیریت واحد نیز وجود ندارد، پس به نظر من بزرگ‌ترین مشکل در حوزهٔ حاکمیت داده آزادسازی داده است.

من فکر می‌کنم امروز در عصری هستیم که یک فرد، ایده، جریان یا فکر داده‌محور بایستی با استقامت و ایستادگی موضوع ملی‌شدن داده‌ها را در کشور عملیاتی و اجرایی نماید.

امروزه تقریباً در محل زندگی و محل کار هر ایرانی یک خط تلفن ثابت وجود دارد، به عبارتی تک‌تک ما با صنعت مخابرات در ارتباط مستقیم هستیم، حتی بخشی از سهام مخابرات سیار در کشور نیز متعلق به شرکت مخابرات ایران است. به عبارت دیگر از منظر خطوط ثابت مخابراتی، ما امروز در منزل تمام ایرانی‌ها حضور داریم و از منظر مخابرات همراه هم، اپراتور همراه اول سهم قابل‌توجهی در بازار اپراتورهای تلفن همراه دارد، لذا در مجموع ما با اکثر عناصر حقیقی و حقوقی کشور در ارتباط هستیم. کلیدی‌ترین شاخصهٔ شرکت مخابرات ایران این است که داده‌های در اختیار این شرکت، داده‌هایی کاملاً معتبر هستند. لوکیشن، شمارهٔ تماس و مشخصات سخت‌افزارهای در اختیار کاربران برای شرکت مخابرات ایران دارایی بسیار بزرگی است و به نظر من مخابرات در آینده می‌تواند در حوزهٔ حاکمیت داده نقش اول و اصلی را بازی کند. البته این بحث از طرفی مسئولیت بزرگی را برای شرکت مخابرات ایران ایجاد

9- Data-enabled

می‌کند، چون داده‌های مردم را در اختیار دارد و اکنون بناست با این داده‌ها برای کشور ارزش‌آفرینی کند. در مقطع کنونی ما نیازمند این هستیم که از فضاهای استارتاپی یا اکوسیستم‌های حوزهٔ نوآوری و شرکت‌های نوپا کمک بگیریم و البته برخی شرکت‌های زیرمجموعهٔ ما این حرکت را به‌صورت جدی شروع کرده‌اند. یکی از بزرگ‌ترین گام‌هایی که بخش فناوری اطلاعات و ارتباطات شرکت مخابرات ایران در دستور کار دارد، بحث حاکمیت داده است و برنامه‌ریزی شده است تا بر این اساس نسل جدیدی از خدمات را به مردم ارائه نماید که در آن داده حرف اول را می‌زند و ارزش داده نیز به‌مرور در بهبود اقتصاد و معیشت مشتریان ایفای نقش خواهد کرد. ما از انقلاب صنعتی چهارم صحبت کردیم در حالی که دنیا به‌سمت انقلاب صنعتی پنجم در حال حرکت است. در انقلاب صنعتی پنجم سه قطب اصلی پایداری، انسان‌محوری و تاب‌آوری وجود دارد. انجام هر کاری در هرکدام از این سه حوزه تا زمانی که تکلیف حاکمیت داده مشخص نشود، امکان‌پذیر نیست. متولیان داده در کشور قبل از هر اقدامی بایستی رابطه و تکلیف بیزینس‌ها و بخش‌های حقوقی، قضایی را با داده مشخص کنند و تا این اتفاق محقق نشود سرمایهٔ هوشمند به‌راحتی به‌سمت استفاده از داده به‌عنوان سرمایه نخواهد رفت. ایجاد جریان هوشمند سرمایه‌گذاری به‌سمت داده نقشی است که حاکمیت داده می‌تواند به‌خوبی ایفا کند. بنابراین با در نظر گرفتن ارکان چشم‌انداز انقلاب صنعتی پنجم، حاکمیت داده نقش اساسی را این تحول ایفا خواهد کرد. این حرف، خواهشی برآمده از دل است، در کشور ما به‌لحاظ مسائل مختلف تاریخی و درگیری در شبکه‌های قدرت، چه داخلی و چه خارجی، در انقلاب‌های صنعتی قبلی عقب‌افتادگی‌های چشمگیری به‌وجود آمد. البته در مقاطعی از تاریخ هم افرادی مثل امیرکبیر می‌خواستند کاری کنند ولی استبداد و استکبار آنها را خفه کردند و در آن مقاطع اتفاقاً کشور ما صدها سال عقب افتاد. حرف پایانی من خواهشی است از تمام مسئولان کشور در حوزهٔ داده و حاکمیت داده، اگر امروز نخواهیم برای انقلاب صنعتی آستین بالا بزنیم چه‌بسا عقب‌افتادگی‌مان بسیار عمیق‌تر از قبل خواهد شد، امروز در نقطهٔ حساسی هستیم و همه باید دست‌دردست هم این راه دشوار را تبیین و تنویر کنیم. در پایان از تمامی اعضای تیم حرفه‌ای تحریریه هم تشکر و قدردانی می‌کنم.»

«داده‌های دربند، بزرگ‌ترین چالش حاکمیت اطلاعات کشور در مسیر ملی‌شدن داده‌ها»

قلمرو دانشی حاکمیت داده[1]

۱- ر.ک.: «ارائه چهارچوبی برای داده‌گان ملی با تمرکز بر توسعه حاکمیت داده» (۱۴۰۰)، نقشینه، ن.، فهیم‌نیا، ف. و احمدیان، ح.، دوفصلنامه علمی فناوری اطلاعات و ارتباطات ایران

هوبان

- تجهیزات رایگان (امانی)
- فاقد هرگونه هزینهٔ پنهان
- به‌روزرسانیِ خودکار سامانه
- بدون نیاز به قرارداد پشتیبانیِ مجزا
- عدم وابستگی به شارژ حجمی اینترنت
- سرعت بالای نصب و راه‌اندازیِ سرویس
- حفظ تصاویر ضبط‌شده حتی در صورت سرقت تجهیزات

https://ivsaas.ir

+۹۸ ۲۱-۲۲۹۴۸۸۶۸
+۹۸ ۲۱-۲۲۹۶۷۷۶۹
www.electronicsecurity.ir
info@electronicsecurity.ir