بسم الله الرحمن الرحیم

معرفی

راه‌حل امن‌سازی شبکه کیهان

شرکت مهندسی پیام‌پرداز

شرکت مهندسی ابل رایان پویا نماینده رسمی شرکت مهندسی ارتباطی پیام پرداز

تیر ماه 1398

فهرست

عنوان **صفحه**

1 مقدمه

امروزه با گسترش فناوری اطلاعات هر سازمان کوچک یا بزرگی دارای یک شبکه کامپیوتری است. در این شبکه‌ها معمولاً سرویس‌دهنده‌های مختلف همچون پایگاه داده، وب سرور، فایل سرور، برنامه‌های کاربردی تحت شبکه به ارائه سرویس به کاربران سازمان می‌پردازند. در محیط‌های سازمانی چندوجهی (غیرمتمرکز)، یک رویکرد دسترسی امن که صرفاً بر پایه یک مدل ایزوله امنیت مبتنی بر شبکه (ایجاد شبکه‌های ایزوله یا حفاظت‌شده) است، دیگر کافی نیست. کسب‌وکار سازمان‌ها و کاربران آن‌ها (کارکنان، پیمانکاران، شرکا و مشتریان) نیاز به دسترسی جامع به مراکز داده، برنامه‌های کاربردی و منابع سازمانی را هم از داخل شبکه سازمان و هم از خارج آن دارند. از طرفی طرز تفکر قدیمی امنیت که تصور می کردند «داخل سازمان = اعتماد» و «بیرون سازمان = غیرقابل‌اعتماد» می‌باشد، در دنیای کسب‌وکار دیجیتال شکسته شده است، باید امکان هر دسترسی در هر زمان و هر مکان و هر دستگاه به خدمات مستقر در داخل سازمان / مرکز داده وجود داشته باشد.

معماری محیط ایزوله تعریف‌شده توسط نرم‌افزار[1] یک مدل قانع‌کننده از مدل **"اعتماد صفر"**[2] را ارائه می‌دهد. این معماری می‌تواند برای اجرای فناوری‌های جدید و مدل‌های جدید کسب‌وکار در طیف وسیعی از صنایع مانند خدمات مخابراتی، بهداشتی، تولیدی و یا خدمات مالی استفاده شود.

این معماری قبل از اعطای دسترسی مستقیم و محافظت‌شده به برنامه‌ها و منابع، یک رویکرد "احراز اصالت و تأیید قبل از اتصال[3]" را پیش‌بینی می‌کند، این مدل دسترسی به معماری شبکه بستگی ندارد و

[1] *Software Defined Perimeter*
[2] *Zero Trust Model*
[3] *Authentication First, Connection Second*

باعث افزایش قابل‌توجه بحث امنیت می‌شود. دسترسی به برنامه را می‌توان به صورت جداگانه هم برای برنامه‌ها و هم برای کاربران محدود کرد. منابع برای تمام کاربران و دستگاه‌ها می‌توانند غیرقابل مشاهده یا غیرقابل‌دسترسی باشند تا زمانی که یک احراز اصالت تمام جانبه صریح، به همراه بررسی انطباق و اعطای مجوز کامل جهت ارائه امنیت مناسب و قابل‌قبول صورت گیرد. در نهایت یک محیط تاریک و پنهان در بستر شبکه به وجود می‌آید که در آن سطح حملات شبکه‌ای کاهش‌یافته است، زیرا هکرها به چیزی که نمی‌توانند ببینند، نمی‌توانند حمله کنند.

دسترسی به شبکه با مدل اعتماد صفر جایگزین تکنولوژی‌های سنتی این حوزه شده است که این مدل به شرکت‌ها اجازه می‌دهد به کارمندان و شرکای خود اعتماد لازم را برای برقراری ارتباط و همکاری امن داشته باشند. با راه‌اندازی شبکه‌هایی با قابلیت اعتماد صفر که **فناوری اطلاعات در سایه** تلقی می‌شود، می‌توانید شرایط را به‌طور کامل مانیتور و کنترل نمایید. این امر به این معنا است که اگر کاربری بخواهد به شبکه ایزوله سازمان راه پیدا کند و از سرویس‌های سازمان استفاده نماید، امکان دسترسی به داده‌ها و منابع شبکه را نخواهد داشت و صرفاً کاربرانی امکان ارتباط با شبکه را دارند که مجوزهای لازم را داشته باشند. شبکه اعتماد صفر، راهی مؤثر برای تقویت امنیت و راهکاری سریع برای جلوگیری از ورودهای غیرمجاز و دسترسی به اطلاعات حساس سازمانی را به وجود می‌آورد.

با توجه به بررسی‌های صورت گرفته در کسب‌وکارهای سازمان‌های مختلف، اطلاعات مفیدی از نحوه نگاه آنان به قضایای مختلف، الزامات و نیازمندی‌های امنیتی سازمان‌ها برای چابکی و توسعه سازمانی استخراج گردید که در ادامه آورده شده است:

- کسب‌وکارهای دیجیتال امروزی نیاز به سیستم، سرویس، داده‌ها و فرآیندهایی دارند که از طریق اکوسیستم‌های مختلف در هر کجا، در هر زمان، از هر دستگاه از طریق اینترنت قابل دسترسی باشد. این مورد سطح حملات به سازمان‌ها را برای مهاجمان افزایش می‌دهد.
- قابلیت دسترسی امن باید تکامل لازم و همه جانبه را برای حالت سیار بودن کاربران، برنامه‌ها و خدمات قابل‌ارائه، داشته باشد.
- آدرس IP و موقعیت مکانی دیگر برای ایجاد اعتماد کافی برای دسترسی به شبکه عملی نیست. مدل باید امکان دسترسی دقیق و هوشیار را فراهم نموده و کمترین ریسک را داشته باشد.
- کسب‌وکارها به دنبال بهبود انعطاف‌پذیری، چابکی و مقیاس‌پذیری خود و انتخاب مدل‌هایی سازگار برای تحقق آن‌ها می‌باشند. این امر اکوسیستم‌های دیجیتال را قادر می‌سازد بدون ارائه خدمات به‌طور مستقیم در اینترنت و بدون وجود خطر حملات معمول مانند انکار سرویس توزیع شوند.

راه‌حل امن سازی شبکه **کیهان** راه‌حلی از شرکت پیام پرداز بر اساس مدل اعتماد صفر (مدل بدون اعتماد) می‌باشد که برای امن‌سازی شبکه کامپیوتری سازمان‌ها مورداستفاده قرار می‌گیرد. در ادامه راه‌حل مطرح‌شده از جوانب مختلف مورد بررسی قرار می‌گیرد.

2 ارزش‌های پیشنهادی

مزایای حاصل از راه‌حل کیهان فوری بوده و همانند یک VPN سنتی، خدماتی که به واسطه راه‌حل کیهان ارائه می‌گردد، دیگر در شبکه عمومی قابل‌مشاهده نیستند و بنابراین از دید مهاجمان محافظت می‌شوند. علاوه بر این، راه‌حل کیهان مزایای قابل‌توجهی در تجربه کاربری، چابکی، سازگاری و سهولت مدیریت سیاست‌های سازمانی را داراست. از طرفی سناریوهای کسب‌وکارهای دیجیتال امروزی که رویکردهای دسترسی سنتی برای آن‌ها مناسب نیستند را امکان‌پذیر می‌سازد. در ادامه تعدادی از موارد استفاده در کسب‌وکارها بر اساس دیدگاه‌های مختلف، مورد بررسی قرار می‌گیرد:

دیدگاه سازمانی:

- ارائه برنامه‌های کاربردی و خدمات به اعضای اکوسیستم کسب‌وکار سازمان، مانند کانال‌های توزیع، تأمین‌کنندگان، پیمانکاران یا خرده‌فروش‌ها و کارمندان راه دور یا کارمندان سیار در کنار محدودسازی دسترسی‌ها به برنامه‌های کاربردی و خدمات دارای مجوز.
- جداسازی برنامه‌های با ارزش سازمانی در داخل شبکه یا ابر برای کاهش تهدیدات داخلی و تأثیر جداسازی آنها بر وظایف محوله برای مدیریت دسترسی‌ها.
- گسترش ارتباطات سازمان در فرایندهای توسعه دفاتر، ادغام‌های سازمانی و ... بدون نیاز به تنظیم مجدد سایت و قوانین فایروال سازمان.
- شفافیت راه‌حل جهت استفاده به عنوان یک راه‌حل واحد برای تمام کاربردها (وب سرورها، برنامه کاربردی اختصاصی سازمان‌ها، برنامه‌های موروثی سازمانی و ...). در صورتی که راه‌حل مورد استفاده برای امنیت با تغییرات شبکه به راحتی تطبیق پیدا کند، محل و نوع شبکه کاربران را محدود نمی‌نماید، لذا هزینه نگهداری را نیز کاهش خواهد داد.
- فعال کردن برنامه‌های سرویسی[4] برای اتصال به سیستم‌های سازمانی و داده‌ها برای فرایندهایی که نیاز به تعامل با شرکت‌ها در محل یا زیرساخت‌ها به عنوان یک سرویس[5] وجود دارد.

[4] *Software as a Service*
[5] *Infrastructure as a Service*

- قابلیت توسعه راه‌حل، در صورتی که در آینده سرورهای حساس دیگری به مجموعه سرورهای محافظت‌شده اضافه شود می‌توان از راه‌حل کیهان برای امن‌سازی ارتباط کاربران با سرورهای حساس جدید (اعم از وب سرور یا سایر برنامه‌های کاربردی Client/Server) نیز استفاده کرد.

دیدگاه امنیتی:

- حذف برنامه‌ها و خدمات از ارائه مستقیم در فضای اینترنت (مخفی سازی سیستم‌ها در شبکه‌های پر خطر برای استفاده در ارتباطات سازمانی و همکاری‌ها).
- دسترسی دقیق (فقط در زمان و فقط به‌اندازه کافی) برای کاربران مجاز برای دسترسی به برنامه‌های خاص و دارای مجوز تنها پس از ارزیابی هویت، چک سلامتی دستگاه و بررسی شرایط کاربر در هنگام اتصال.
- فعال کردن دسترسی، مستقل از مکان فیزیکی کاربر یا آدرس IP دستگاه (به جز مواردی که سیاست ممنوع است. برای مثال در مناطق خاص جهان). سیاست‌های دسترسی بر اساس هویت کاربر، دستگاه، برنامه کاربردی و شبکه اتصالی با توجه ویژه به الزامات احراز اصالت قوی و حفاظت از نقطه پایانی.
- اعطای دسترسی فقط به برنامه‌ها/سرویس‌های خاص، نه کل شبکه. این مورد باعث می‌شود در نیاز به دسترسی بیش از حد به تمام پورت‌ها، پروتکل‌ها و یا تمام برنامه‌های کاربردی که برخی از آن‌ها ممکن است برای کاربران مجاز نباشد، محدودیت ایجاد شود.
- محرمانگی[6] و صحت[7] داده‌های مبادله شده. فراهم نمودن رمزنگاری کامل اطلاعات حساس مبادله شده بین کاربر و سرویس‌دهنده با روش‌های مدرن رمزنگاری جهت جلوگیری از امکان شنود اطلاعات، استراق سمع و ...
- ارائه بازرسی اختیاری از جریان‌های ترافیکی برای فعالیت‌های غیرمعمول و خطرساز بیش از حد در قالب دسترسی به اطلاعات حساس و اجرای نرم‌افزارهای مخرب.
- فعال کردن نظارت اختیاری کاربران برای نشان دادن فعالیت‌های غیرمعمول، مدت زمان اتصال و یا پهنای باند مورداستفاده.

---

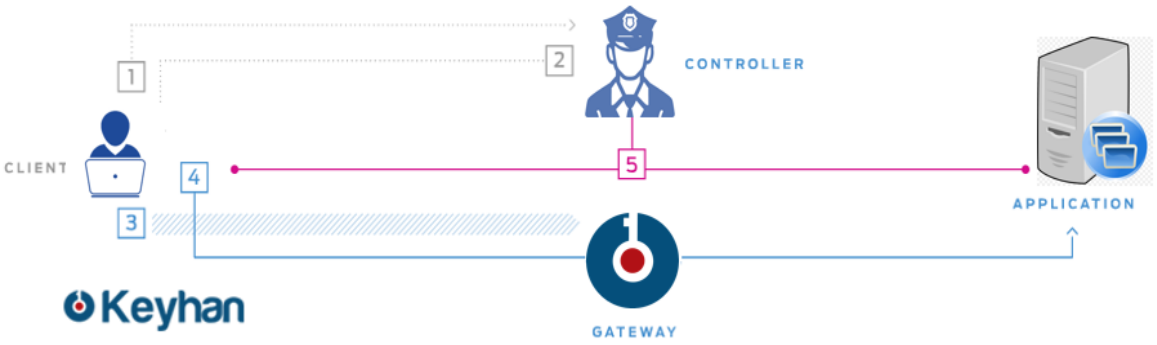
[6] *Confidentiality*
[7] *Integrity*

دیدگاه کاربری:

- ارائه یک تجربه کاربری مناسب به کاربران برای دسترسی به برنامه‌ها و سرویس‌های سازمانی صرف‌نظر از محل شبکه بدون تغییر در تجربه کاربر برای دسترسی به برنامه‌ها. در این حالت تمایزی بین حضور/عدم حضور کاربر در شبکه سازمان وجود ندارد.
- تأیید هویت کاربران در دستگاه‌های شخصی. راه‌حل کیهان می‌تواند امنیت و استفاده از وسایل همراه[8] را بهبود بخشد با کاهش نیاز به مدیریت کامل و ساده‌سازی امکان دسترسی مستقیم به برنامه‌های کاربردی سازمان.

3 نحوه کار

معماری نرم‌افزاری کیهان از سه جزء اصلی تشکیل‌شده است: کاربر، کنترلر (کنترل کننده) و دروازه ورودی. کنترل کننده مغز سیستم بوده و به عنوان یک کارگزار اعتماد برای سیستم عمل می‌کند. کنترل کننده تمام شرایط را بررسی و سپس مجوز را اعطا می‌نماید. نحوه کار سیستم به صورت زیر می‌باشد:



1. نرم‌افزار کاربری با استفاده از پروتکل احراز اصالت، درخواست دسترسی و تأیید هویت کاربر را به کنترل کننده ارسال می‌نماید.
2. کنترل کننده اصالت و اعتبار کاربر را ارزیابی نموده و در صورت تایید، سیاست‌های دسترسی را بر اساس نقش کاربر، قوانین تعریف‌شده و شرایط محیطی کاربر ساخته و مجوزهای دسترسی را به کاربر واگذار می‌نماید.
3. کاربر بر اساس مجوزهای تخصیص داده‌شده از طریق دروازه به منابع سازمان دسترسی پیدا می‌نماید.

[8] *BYOD*

4. یک بخش پویا از شبکه برای این جلسه ساخته‌شده است. پس از اعطای مجوز، تمام دسترسی به منابع از کاربر تا سرور/سرویس سازمان در تونل به صورت رمزگذاری شده و از طریق دروازه به سرور منتقل می‌شود. کلیه اتصالات کاربر به سامانه از طریق سرویس رویداد نگاری، ثبت می‌گردد. حصول اطمینان از رعایت دائمی و قابل‌اطمینان از دسترسی‌ها و شرایط کاربر در این صورت امکان‌پذیر می‌باشد.
5. کنترل کننده به طور مداوم بر تغییرات شرایط کاربر و وضعیت او نظارت نموده و در صورت لزوم عکس‌العمل نشان می‌دهد.

4 ویژگی‌های راه‌حل

راه‌حل کیهان یک محیط امن، یکپارچه و پیکربندی شده را بین دستگاه‌های کاربر و منابع ایجاد می‌نماید. این روش انعطاف‌پذیر و با فرض اعتماد صفر، مزایایی فراوانی را نسبت به معماری‌های سنتی ارائه می‌دهد: احراز هویت و مجوز از طریق سیاست‌ها اعمال می‌شود، کنترل دسترسی قانونمندتر و قابل تنظیم است و منابع را می‌توان از بردارهای حملات خارجی یا داخلی پنهان کرد. در ادامه به بررسی مزایای این راه‌حل در قالب 4 عنوان اصلی زیر پرداخته شده است:

۱-تأیید اعتبار و مجوز | ۲- محدودسازی دسترسی و اجرای سیاست | ۳- اتصال و مدیریت | ٤- نظارت بر رفتار کاربران مجاز

4-1 تأیید اعتبار و مجوزها – Authentication & Authorization

- **تأیید اعتبار و مجوزها قبل از اتصال[۹]**

قبل از هر نوع اتصال، بررسی هویت کاربر، دستگاه، شبکه و محیط کاری باید انجام و تأییدیه‌های لازم گرفته شود. پس از تأیید اعتبار موفقیت‌آمیز، یک سطح مشخص اعتماد ایجادشده است که به برنامه کاربردی

[۹] *Authenticate and Authorize before connecting*

دارای مجوز یا دسترسی به منابع منجر می‌شود. دسترسی بر اساس کاربر، دستگاه و زمینه کاربرد مانند زمان روز، مکان جغرافیایی، نقش کاربر، مشخصات دستگاه و انطباق آن صورت می‌گیرد.

- **تأیید هویت چند عاملی**[10]

فراهم نمودن ابزارهای متنوع احراز اصالت برای کاربران مانند توکن‌های نرم‌افزاری، سخت‌افزاری، SMS-OTP و... در این حالت سازمان می‌تواند بسته به شرایط استفاده و نوع کاربران روش مناسبی را انتخاب نماید.

- **تفکیک وظایف کاربر با مجوزها/ اعطای مجوز بر اساس نقش یا قلمرو**

با فراهم نمودن کنترل مجوزهای دسترسی کاربران بر اساس مجاری مختلف و پشتیبانی از تقسیم‌بندی میکرو، کاربران ممکن است با مجوزهای متنوع و دارای سطح مختلف از دستگاه‌ها، اعتبارنامه‌های کاربری مختلف برای دسترسی به بخش‌های مختلف مجاز و غیرمجاز، استفاده نمایند. این مورد همچنین امکان اجرای کنترل‌های متفاوت برای فروشندگان و انواع کاربران پیمانکار که نیاز به دسترسی به منابع و برنامه‌های خاص را دارند، فراهم می‌نماید. کاربران می‌توانند گروه‌بندی شوند، از جمله کاربران دارای امتیاز، برای فعال کردن یا جلوگیری از دسترسی به کلاس‌های مختلف برنامه‌ها و منابع. این باعث کاهش سربار اداری مدیریت کاربران و برنامه‌های فردی می‌شود.

- **بررسی سلامتی سیستم کاربر**[11]

امکان چکاب سلامت امنیت سیستم کاربران قبل از اتصال به سامانه از لحاظ مواردی مانند مشخصات سیستم‌عامل، مشخصات آنتی ویروس، مشخصات فایروال برای جلوگیری از اتصال سیستم‌های ناسالم از دید مدیر سامانه به شبکه سازمان وجود دارد. دستگاه‌های خارج از انطباق می‌توانند توسط مدیر مورد رویداد نگاری، هشدار دهی و یا جلوگیری از دسترسی گردند.

4-2 دسترسی و اجرای سیاست – Access & Policy Enforcement

- **کنترل دسترسی با ریزدانگی بالا**

[10] *MFA*
[11] *Host Checking*

رویکرد کنترل دسترسی کاربران با ریزدانگی بالا به برنامه‌ها، منابع یا زیر بخش‌های سازمان جهت پشتیبانی از جداسازی کاربران خارجی (شرکا، مشتریان) از کاربران داخلی (کارکنان، پیمانکاران) و کاربران ممتاز (مدیر، DevOps، دانشمندان داده) که در صورت نیاز در هنگام اتصال از طریق سیاست‌ها فراهم می‌گردد.

- **سیاست دهی و اجرای یکنواخت**

ایجاد مدل سیاستی یکپارچه و اجرایی یکنواخت. این امر در مورد هر دو دسته کاربران داخلی و خارجی، دستگاه‌های آن‌ها و همچنین برای مرکز داده داخلی (ابر خصوصی) و ابر عمومی کاربرد دارد.

- **سیاست دهی و پیکربندی متمرکز**

با تمرکز و ادغام اطلاعات سیاست و پیکربندی، در تمام مواردی که پیاده‌سازی سیاست‌های ارتباطی و دسترسی نیاز، هماهنگی بیشتری را به همراه دارد. این امر باعث کاهش خطاهای دستی یا انسانی شده، مانع پیکربندی نادرست و عدم رعایت خط‌مشی سازمان و در نهایت منجر به سطح بالاتری از امنیت می‌گردد.

3-4 اتصال و مدیریت- Connectivity & Management

- **اتصال مبتنی بر نیاز و بر اساس تقاضا**[12]

بیان عباراتی تحت عنوان Dark Site یا Dark Cloud که خدمات یا منابع به‌طور کامل و ایزوله شده از اتصالات و دسترسی‌های داخلی و یا خارجی پنهان باقی می‌ماند. سرویس درخواست اتصالی را قبول نخواهد کرد تا زمانی که یک کاربر و دستگاه را به‌طور مرکزی تأیید و مجاز تشخیص دهد. مزیت اضافه روش تأیید اعتبار قبل از اتصال، این است که خسارت حملات DDOS به‌سادگی با کاهش (قطع کردن) اتصال برای درخواست‌کنندگان غیرمجاز حذف می‌گردد.

اتصال یک به یک، بر اساس تقاضا، با استفاده از یک مدل شبکه پوشش داده می‌شود. تقسیم‌بندی میکرو[13] برای برنامه‌ها، منابع و دسترسی منحصربه‌فرد اعمال می‌شود. انواع مختلفی از اتصالات امن را می‌توان به صورت پویا با توجه به نیاز برنامه‌های کاربردی یا منابع تعیین نمود.

- **شفافیت**

[12] *On-demand connections*
[13] *Micro segmentation*

سیستم کیهان در لایه شبکه عمل کرده و از دید لایه کاربرد کاملاً شفاف است. بنابراین نیازی به تغییر در برنامه‌های کاربردی وجود نخواهد داشت. همچنین هیچ تغییری در سایر کاربردهای مورداستفاده کاربر رخ نخواهد داد.

4-4 نظارت بر رفتار کاربران مجاز – Privileged users under magnifier

- **رویداد نگاری**

سامانه کیهان با تهیه رویداد از اتفاقات سیستم می‌تواند کمک شایانی در ردگیری فعالیت‌های کاربر ارائه نماید. در موقع اتصال کاربر به سرور کیهان، نام کاربری، آدرس IP کامپیوتر، نام دامنه، نام کاربر واردشده به سیستم‌عامل و شناسه یکتای ماژول کاربر و ... در سیستم ثبت می‌شوند. بنابراین با توجه به مکانیسم احراز اصالت قوی کیهان و رویداد نگاری انجام‌شده، معیار انکارناپذیری به خوبی برآورده می‌گردد. در حقیقت در سیستم کیهان امکان سوءاستفاده از هویت کاربر توسط سایر اعضا و حتی مدیر وجود نخواهد داشت.

- **امکان تحلیل ترافیک ارسالی کاربران**

سامانه کیهان مجهز به سیستم تحلیل ترافیک ارسالی کاربران می‌باشد. این سرویس که به صورت محصول جداگانه قابل‌عرضه می‌باشد. امکان تهیه گزارشات متنوع از میزان و نوع دسترسی‌های کاربران به سرورهای تحت حفاظت را برای مدیر سیستم فراهم می‌آورد.

- **ردگیری فعالیت‌های کاربر**

به منظور پیش‌گیری از وقوع اقدامات خلاف توسط کاربران و نیز تشخیص و ردگیری این‌گونه فعالیت‌ها در صورت وقوع، سیستم‌های اطلاعاتی کلیه فعالیت‌های انجام‌گرفته را رویداد نگاری کرده و آن‌ها را در اختیار مدیر سیستم قرار می‌دهند. بسته به سطح رویداد نگاری و جزییات موردنظر، ممکن است عملیات ردگیری توسط برنامه‌های کاربردی و یا تجهیزات شبکه انجام گیرد.

- **تشخیص حملات رایج و شناخته‌شده دارای امضاء**

امروزه، ابزارهای نفوذ و حمله به سرویس‌های مختلف کامپیوتری و شبکه‌ای به‌وفور یافت می‌شود و چگونگی استفاده از آن‌ها، نیاز به داشتن دانش تخصصی زیاد ندارد. ازاین‌رو، امکان استفاده از این ابزارها برای افراد بسیاری با هر انگیزه‌ای (انگیزه‌های مالی، سرگرمی و یا خصومت شخصی یا سازمانی) فراهم آورده است. انواع حملاتی که علیه این سرویس‌ها انجام می‌شود شامل از کار اندازی

سرویس یا شبکه، شناسایی و استخراج غیرمجاز اطلاعات، دست‌کاری داده‌ها و تنظیمات، دور زدن مکانیسم‌های کنترل دسترسی، عبور ترافیک غیرمجاز، شنود اطلاعات، تقلب، سرقت اطلاعات مالی، آلوده کردن سیستم‌ها به بدافزار و غیره می‌باشد. برای پاسخگویی به چالش‌های ذکرشده، استفاده از سامانه تشخیص نفوذ و پایش کامل خروجی‌های آن توصیه می‌شود.

- **تحلیل ناهنجاری ترافیک عبوری کاربران راه دور**

امکان تشخیص تلاش‌هایی که برای حمله به زیرساخت شبکه یا سرویس‌ها و با استفاده از روش‌های شناخته‌شده صورت می‌پذیرد را با استفاده از ابزارهایی نظیر سیستم‌های تشخیص نفوذ خواهند داشت. برخی از حملات و تهدیدات، با استفاده از روش‌های ناشناخته انجام خواهد شد و تنها روشی که می‌توان آن‌ها را شناسایی کرد، تحلیل ناهنجاری‌های جریان ترافیک و بررسی آثار فعالیت‌های نفوذگر بر روی جریان شبکه است. هدف از به‌کارگیری سیستم تحلیل ناهنجاری جریان ترافیک، تشخیص حملاتی است که دارای ویژگی‌های رفتاری خاص هستند و به دلیل ناشناخته بودن الگوی آن‌ها، هنجار بودن محتوای آن‌ها و یا گسترده بودن سطح حمله، قابل‌تشخیص در سیستم‌های تشخیص نفوذ سنتی نیستند.

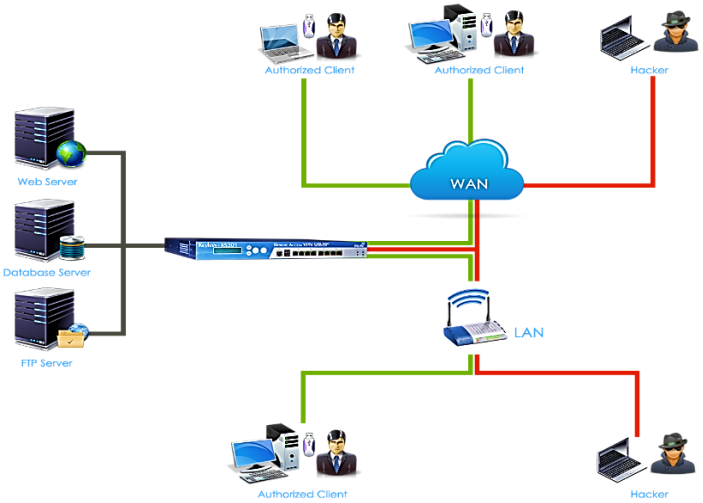
- **دستور پذیری سامانه**

امکان ارسال دستور از سرور تحلیل رویداد و ترافیک به سامانه کیهان، در صورت تشخیص نقض نمودن قوانین و الزامات امنیتی سازمان توسط کاربران مجاز وجود دارد. در این حالت کاربر غیرفعال و کلیه دسترسی‌های آن گرفته می‌شود و به مدیر سامانه وضعیت نمایش داده‌شده تا به آن رسیدگی نماید. در این صورت مدیران سازمان مطمئن می‌گردند که وضعیت کاملاً تحت کنترل و نظارت مستمر بوده و در صورت بروز اتفاق مشکوکی از سمت کاربران، اوضاع به صورت خودکار توسط سامانه‌ها و بدون دخالت انسان مدیریت می‌گردد.

5 سناریو استفاده

به عنوان مثال فرض کنید سازمانی به دنبال برقراری امکان ارتباط راه دور کارمندان سازمان (کارمندان داخلی، دفاتر سطح کشور) و پیمانکاران (شرکای تجاری، همکاران فنی) به شبکه سازمان با دسترسی محدود می‌باشد. کارکنان راه دور و پیمانکاران نیاز به دسترسی به سیستم‌های حیاتی سازمان را از هر نقطه و هر دستگاهی دارند. در این حالت سامانه کیهان بدین صورت عمل می‌نماید که عموماً سرویس‌دهنده کیهان

در جلوی سرویس‌دهنده‌های حساس سازمان قرار داده می‌شود و بر روی هر یک از کامپیوترهای کارمندان سازمان، نرم‌افزار کلاینت کیهان نصب می‌شود. جهت امکان بهره‌برداری کاربران از سرویس‌دهنده‌های حیاتی، ابتدا لازم است تا مدیر سیستم، کاربران و حق دسترسی آنان به هر یک از بخش‌های مزرعه سرور را مشخص نماید و برای هر کاربر یک توکن امنیتی برنامه‌ریزی نماید.



هر یک از کارکنان (اعم از داخل سازمان و خارج از سازمان) **تنها** با استفاده از نرم‌افزار کلاینت کیهان و اجرای یک پروتکل احراز اصالت دوطرفه و به صورت دو عاملی قادر خواهند بود با دستگاه کیهان سرور احراز اصالت بشوند. با انجام موفقیت‌آمیز فرآیند احراز اصالت دوسویه کاربر و سرور، یک تونل امن (VPN) بین کامپیوتر کاربر و سرور کیهان برقرار می‌شود که کلیه داده‌های مبادله شده درون آن رمز می‌گردد. بدین ترتیب سرویس‌های محرمانگی و صحت تأمین می‌شود و اطلاعات مبادله شده کاربران با سرورهای تحت حفاظت از گزند حملات شبکه‌ای مانند استراق سمع، تکرار، تغییر، شخصی در میان[14] و ... در امان می‌مانند. کیهان سیاست‌ها و مجوزهای را بر اساس هویت کاربر اعطا نموده و از این طریق باعث کاهش سطح حمله و محدود کردن کاربران به آنچه باید ببینند می‌شود. این نه‌تنها اطمینان می‌دهد که کاربران تنها به آنچه مجاز به مشاهده هستند دسترسی دارند، بلکه تجربه کاربر راه دور را از لحاظ عملکرد بهبود می‌بخشد. سرور کیهان همچنین به عنوان یک دیواره آتش قوی عمل کرده و از نفوذ افراد غیرمجاز و بد افزارها به

[14] *Man in the middle*

سرویس‌دهنده‌ها جلوگیری می‌نماید. بدین ترتیب امکان انجام حملات ممانعت از سرویس (DoS) بر روی سرویس‌دهنده‌های حیاتی توسط نفوذ گران از میان خواهد رفت.

6 مزایای مشهود در کسب‌وکار

6-1 صرفه‌جویی در هزینه و کار

- جایگزینی اجزای سنتی امنیت شبکه، هزینه‌های صدور مجوز و پشتیبانی را کاهش می‌دهد. حتی یکپارچه‌سازی این اجزای سنتی برای ارائه ارزش، باعث کاهش هزینه‌ها می‌گردد.
- پیاده‌سازی و اجرای سیاست‌های امنیتی با استفاده از راه‌حل کیهان، پیچیدگی عملیاتی و وابستگی به ابزارهای امنیتی سنتی را کاهش می‌دهد.
- کاهش هزینه‌ها با جایگزینی MPLS یا استفاده از خطوط اجاره‌ای، سازمان‌ها می‌توانند با ایجاد شبکه مجازی خصوصی خود در ستون فقرات یک شبکه عمومی هزینه‌ها را کاهش دهند یا حذف نمایند.

6-2 افزایش چابکی عملیات IT

در بسیاری از موارد، سیستم‌های اطلاعاتی و فرآیندهای IT به عنوان پوشش فرایندهای تجاری عمل می‌کنند. پیاده‌سازی این‌گونه راه‌حل‌ها می‌تواند به‌طور خودکار توسط رویدادهای IT هدایت شود. این مورد فناوری اطلاعات را تسریع می‌بخشد و به خواسته‌های کسب‌وکار و امنیت مناسب پاسخ می‌دهد.

6-3 کاهش ریسک و افزایش سازگاری سامانه‌ها در سطح سازمان

در مقایسه با رویکردهای سنتی خطرها را کاهش داده و باعث سرکوب تهدیدها و کاهش سطح حملات، جلوگیری از حملات مبتنی بر شبکه و بهره‌برداری از آسیب‌پذیری‌های برنامه‌ها و سرورها می‌گردد. همچنین به سیستم‌های GRC[15] (مانند SIEM) پاسخ داده تا عملیات تطابق را برای سیستم‌ها و برنامه‌های کاربردی ساده‌تر نمایند.

[15] Governance, Risk Management, and Compliance

6-4 کوچک نمودن محدوده تحت نظارت

سازگاری با جمع‌آوری داده‌ها و گزارش دهی و انجام ممیزی‌های مربوطه، زیرا کنترل اتصالات کاربران را در دستگاه‌های ثبت‌شده به برنامه‌های کاربردی/سرویس‌های خاص متمرکز می‌کند. تقسیم‌بندی شبکه‌های کوچک ارائه‌شده اغلب برای کاهش دامنه تطابق استفاده می‌شود که می‌تواند تأثیر بزرگ و مثبتی بر روی تلاش‌های گزارش دهی داشته باشد.

6-5 انطباق با رایانش ابری امن

راه‌حل کیهان می‌تواند به سرعت، با اطمینان و ایمن ساختارهای ابری را با کاهش هزینه‌ها و پیچیدگی معماری امنیت موردنیاز برای پشتیبانی از برنامه‌های کاربردی در ابر عمومی، ابر خصوصی، مرکز داده یا محیط‌های مخلوط، کمک نماید. این مدل زمان مشاهده مزایای استفاده از ابر را به صورت محسوس کاهش می‌دهد، زیرا برنامه‌های کاربردی را می‌توان سریع‌تر با موقعیت امنیتی معادل یا بهتر در مقایسه با راه‌حل‌های موجود و البته پرهزینه به کار برد.

6-6 فراهم‌سازی قابلیت انعطاف‌پذیری کسب‌وکارها و نوآوری

ارائه یک معماری امن، کسب‌وکار را قادر می‌سازد تا تغییرات کسب‌وکار و راهکارهای جدید خود را سریعاً و ایمن در اولویت‌های کاری خود قرار دهد.

مثال‌ها:

- امکان اجرای ضرورت کسب‌وکار برای انتقال مرکز تماس داخلی به مرکز تماس خانگی
- امکان برون سپاری کارکردهای غیر هسته‌ای به اشخاص ثالث
- امکان راه‌اندازی کیوسک‌های مشتری در شبکه‌های محلی و شبکه‌های شریک ثالث راه دور و ایجاد یک خط جدید از کسب‌وکار
- امکان استقرار دارایی‌های شرکت بر روی سایت‌های مشتری، در کنار فراهم نمودن امکان ایجاد یکپارچه‌سازی قوی با مشتریان و ایجاد درآمد جدید

7 نتیجه‌گیری

ما در دوران جنگ سایبری زندگی می‌کنیم، با این حال بحث اعتماد در تمام سطوح از کاربران سازمان تا دستگاه‌ها و شبکه‌ها معمولاً فرض شده است و این عامل می‌تواند باعث بروز خسارات سنگینی برای سازمان‌ها گردد. امنیت محیط استاتیک سنتی شبکه‌های سازمانی، غیر پاسخگو و غیرمتمرکز است. این یک حس اعتماد ناکافی را برای ما به همراه دارد و هرلحظه احتمال ایجاد رخدادی امنیتی در سازمان وجود دارد. مدل اعتماد صفر با هدف ارتقاء مکانیسم‌های دسترسی امن جهت اطمینان از شناسایی، انطباق و اتصال به‌طور مستقیم بین کاربران، دستگاه‌ها و برنامه‌ها / منابع نگهداری شده در مراکز داده یا ابر بیان می‌گردد. در اصل، راه‌حل‌های امن دسترسی **محصول کیهان**، ارائه‌دهنده قابلیت‌های مدل اعتماد صفر برای افزایش سطح اعتماد و امنیت در کنار کاهش ریسک در انجام کسب‌وکار سازمان می‌باشد.

راه‌حل‌هایی همچون راه‌حل کیهان بر اساس معماری محیط ایزوله تعریف‌شده توسط نرم‌افزار مزایای امنیتی فزاینده‌ای مانند ارائه منابع تاریک/پنهان به هکرها، امکان اتصال همیشگی بنا به درخواست کاربر، افزایش انعطاف‌پذیری شبکه و انعطاف‌پذیری و کاهش نفوذ نرم‌افزارهای مخرب را ارائه می‌دهد. با این حال، این بدان معنی نیست که دیگر مدل‌های دسترسی امن باید حذف شوند یا در حال حاضر نامعتبر هستند. همه سناریوها یا منابع نیازی به یک سیاست واقعی مبتنی بر اعتماد ندارند. برنامه‌های کاربردی مختلف یا کلاس‌های اطلاعات می‌توانند به طیفی از سطوح اعتماد که باید در هر یک از سیاست‌های دسترسی امن ایجاد شوند، به منظور دسترسی محافظت‌شده، نقشه‌برداری شوند.

با اطمینان می‌توان بیان نمود که راه‌حل محصولی کیهان دارای تجربه، راه‌حل‌های متنوع و قابلیت‌هایی است که می‌تواند تفکر اعتماد صفر و مدل‌های ترکیبی امنیتی را فعال نموده تا سازمان‌هایی که به دنبال افزایش چابکی نیروی کار، افزایش پاسخگویی به نیازهای کسب‌وکار و تجارت در کنار افزایش امنیت و انطباق با کاهش سطوح ریسک و افزایش اطمینان و اعتماد موردنظر هستند، بتوانند نیازهای خود را برآورده نمایند.

8 معرفی شرکت

راه‌حل ارائه‌شده (محصول کیهان) به‌منظور ارائه راهکاری جامع جهت امن سازی ارتباطات شبکه‌ای سازمان‌ها توسط شرکت مهندسی **پیام پرداز** تهیه‌شده است. این شرکت با بیش از دو دهه سابقه فعالیت مستمر، به عنوان یک شرکت پیشرو در زمینه خدمات مشاوره، طراحی و اجرای امنیت فضای تبادل اطلاعات شناخته‌شده و در حال حاضر دارای سبدی متنوع از محصولات حوزه امنیت فناوری اطلاعات است.