شرکت کامپیوتری
علم و صنعت

تلفن: ۰۲۱۸۴۳۳۶ – داخلی ۴۴۰
ایمیل: CyberSecurity [AT] elmosanat.com
نشانی وب سایت: www.elmosanat.com
نشانی دفتر مرکزی: تهران، خیابان فاطمی، خیابان پروین اعتصامی، پلاک ۳

شرکت علم و صنعت

ارائـه کننده راهکارهـای نوین امنیـت فناوری اطلاعات

راهکارها و خدمات امنیت فناوری اطلاعات علم و صنعت >

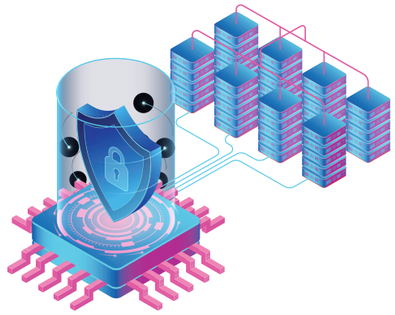
راهکار های علم وصنعت

مهم ترین عامل موثر در حفظ امنیت دارایی‌های اطلاعاتی و نیز پیشگیری از اختلال عملکرد سرویسهای سازمانی، واکنش هماهنگ و یکپارچه راهکارهای حفاظتی می باشد. راهکارهای حفاظتی علم و صنعت ترکیبی هماهنگ از محصولات و خدمات ویژه منطبق با استانداردهای امنیت فناوری اطلاعات بوده که علاوه بر کاهش هزینه های اجرایی و نگهداری، امکانات امنیتی فراگیر را در اختیار شما قرار می دهد.

راهکار امنیت نقاط پایانی

حفاظت از ایستگاه های کاری و سرورها در برابرانواع تهدید ها

- مقابله با انواع بدافزار در سراسر شبکه
- پیاده سازی فناوری های امنیتی پیشرفته جهت شناسایی و دفع تهدیدها
- پوشش کامل امنیتی برای حفاظت از سیستمهای حساس و آسیب پذیر
- شناسایی مستمر و رفع نقاط ضعف و آسیب‌پذیر
- آگاهی رسانی و انتقال دانش مقابله با انواع بدافزار
- برنامه ریزی و آمادگی برای مقابله با حملات سایبری



راهکار امنیت پیشرفته

واکنش هماهنگ در برابر تهدیدهای داخلی و خارجی

- شناسایی نقاط ضعف و انتخاب کارآمدترین راهکارهای مقابله با تهدید ها
- کنترل سطح دسترسی به سرویسها و منابع شبکه
- راه اندازی راهکارهای امنیتی سازگار با چرخش کار سازمان
- پیاده سازی روشهای عبور از بحرانهای امنیتی
- برقراری امنیت در لایه های مختلف شبکه
- آموزش راهبران و کاربران برای مقابله با تهدید ها

راهکار امنیت جامع

شکار تهدید های پیشرفته و واکنش دفاعی خودکار

- ارزیابی مستمر وضعیت امنیت شبکه و رفع آسیب‌پذیری ها
- تهیه نقشه راه امنیت و طراحی مراحل و استراتژی دفاعی
- پیاده سازی سامانه رصد و واکنش خودکار در برابر حملات
- پالایش رخدادها بمنظور شناسایی و پیشگیری از حملات روز صفر
- پوشش امنیتی بسترها و زیرساخت مجازی

راهکار پیشگیری از نشت اطلاعات

امنیت دارایی های اطلاعاتی ارزشمند و حیاتی

- شناسایی و دسته بندی اطلاعات حساس
- کنترل راه های تبادل اطلاعات
- طراحی سیاست های حفاظت از اطلاعات مهم سازمانی
- پیاده سازی و راه اندازی سامانه پیشگیری از نشت اطلاعات
- بررسی رفتار کاربران و پیشگیری از سرقت و یا تغییر اطلاعات
- کنترل سطح دسترسی برنامه ها به اطلاعات حساس

راهکار امنیت نقاط پایانی

ایستگاه های کاری، سرورها و سایر دستگاه هایی که در ارتباط با یکدیگر بعنوان نقاط پایانی اجزای یک شبکه را تشکیل می دهند، به دلیل در اختیار داشتن منابع مهم از جمله سرویسها و دارایی های اطلاعاتی سازمان، همواره از جمله اهداف اصلی سوء استفاده و نفوذ محسوب می شوند.

چالشهای گوناگونی برای حفاظت از نقاط پایانی و حفظ تداوم عملکرد صحیح آنها مطرح می باشد که در صورت عدم توجه و رسیدگی به هر یک از آنها، تدابیر حفاظتی و دفاعی اندیشیده شده بمنظور حفظ امنیت شبکه را کم اثر کرده و امکان نفوذ انواع تهدیدها از جمله بدافزارها را فراهم می سازد.

راهکار امنیت نقاط پایانی علم و صنعت، خدمات و محصولات مورد نیاز جهت رفع چالشهای فوق را درقالب راهکاری یکپارچه بمنظور حفاظت از نقاط پایانی برای شما فراهم نموده است.

- ارزیابی ابتدایی بمنظور سنجش نیازمندیها و شناسایی نقاط ضعف و آسیب پذیر
- بازنگری طراحی امنیت بر مبنای استانداردهای معتبر
- راه اندازی و نگهداری سامانه های مدیریت نصب اصلاحیه و آسیب پذیری
- ارزیابی دوره ای وضعیت امنیت نقاط پایاتی و کنترل عملکرد محصولات امنیتی
- خدمات مشاوره بمنظور انتخاب محصولات امنیتی سازگار و فناوریهای کارآمد
- پیکربندی زیرساختها و سرویسهای مرتبط با نقاط پایانی
- پیاده سازی، راه اندازی و نگهداری سامانه یکپارچه ضدبدافزار
- خدمات پشتیبانی نامحدود

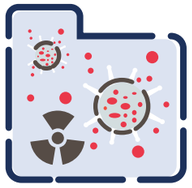
چالشهای امنیتی در لایه نقاط پایانی

مشکل به روز رسانی

سوء استفاده از نقاط آسیب پذیری ها

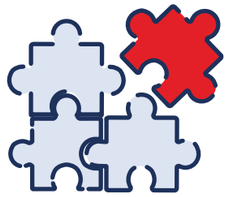
طراحی ناکارآمد سطوح امنیت

سهولت نفوذ تهدیدها و دسترسی آسان به نقاط آسیب پذیر



حملات بدافزارها

فعالیت مخرب انواع ویروس، باج افزار، جاسوس افزار و تهدیدهای پیشرفته و ماندگار



ناسازگاری محصولات امنیتی

کندی عملکرد نرم افزارها و تاثیر منفی بر سرعت کار

راهکار امنیت پیشرفته

برای حفاظت کامل از تمام اجزای یک شبکه که متشکل از نقاط پایانی، سرورها و سرویس ها، بستر مجازی و زیرساخت ارتباطی می باشد، شناسایی نقاط آسیب پذیر و حیاتی بمنظور طراحی ساختار یکپارچه امنیت بر اساس استاندارد های معتبر و فناوری های نوین، گامی کلیدی محسوب می شوند.

در پیاده سازی راهکارهای پیشرفته امنیت، علاوه بر لزوم پیش بینی انواع چالشهایی که بطور خاص زیرساخت فناوری اطلاعات را تهدید می کنند، باید تعامل و هماهنگی بین راهکار های حفاظتی برقرار گردد؛ تا سامانه‌های دفاعی بطور هماهنگ قادر به شناسایی حملات و نیز واکنش در برابر رخداد ها باشند.

بهره مندی از دانش و مهارت متخصصان مجرب و با سابقه، عامل اصلی موفقیت ما در طراحی، پیاده سازی و نگهداری پروژه های بزرگ راهکارهای نوین امنیتی می باشد.

حملات پیشرفته

اختلال وسیع در سامانه ها و چرخش کار

نقاط ضعف قابل شناسایی

نفوذ به سرویسها و منابع حیاتی شبکه

دسترسی های غیر مجاز

ورود نفوذگران بمنظور شناسایی آسیب پذیریها

به خطر افتادن اطلاعات حساس

باجگیری و یا تخریب داده ها توسط نفوذگران

محصولات امنیتی ضعیف

انتشار وسیع بدافزار در سطح شبکه

ایمیلها و وب سایت های جعلی

فریب کاربران برای اجرای کد مخرب و یا سرقت اطلاعات

توقف سرویس ها و چرخش کار

ضرر و زیان مالی و اعتباری همراه با خسارتهای وسیع

ضعف در دانش و تجربه

آماده نبودن نیروها جهت واکنش هماهنگ در برابر تهدید ها

سیاست های دفاعی ناکارآمد

فقدان برنامه مشخص برای مقابله با رخدادهای امنیتی

- ارزیابی امنیت نقاط پایانی، سرویسها، شبکه داخلی، بستر ارتباطی و زیر ساخت مجازی
- طراحی و بازنگری ساختار امنیت شبکه بر مبنای استانداردهاو سیاستهای سازمانی
- نصب و راه اندازی و پیکربندی سامانه مدیریت جامع تهدید ها
- پیاده سازی راهکار جامع مدیریت سطح دسترسی
- نصب و راه اندازی ضدهرزنامه
- مستند سازی پیکربندی های اعمال شده در محصولات
- برگزاری دوره های آموزشی و آگاه سازی
- ارائه خدمات مشاوره بمنظور انتخاب محصولات امنیتی مورد نیاز
- نصب و راه اندازی راهکار مدیریت آسیب پذیری
- نصب و راه اندازی راهکار مدیریت متمرکز پشتیبانی اطلاعات
- پیاده سازی سامانه یکپارچه ضدبدافزار
- پیاده سازی راهکار مدیریت نصب اصلاحیه
- بررسی دوره ای عملکرد محصولات امنیتی و وضعیت امنیت زیرساخت فناوری اطلاعات
- واکنش به رخدادها و خدمات پشتیبانی نامحدود

راهکار امنیت جامع

راهکار امنیت جامع بر مبنای شناخت صحیح چالشهای حفاظتی، نیازهای مطرح شده در برقراری امنیت را پوشش داده و با ایجاد یکپارچگی بین محصولات امنیتی، امکان واکنش سریع و خودکار در برابر تهدیدهای پیشرفته و پیچیده را فراهم می‌سازد.

مهمترین عامل در حفظ یکپارچگی و هماهنگی در واکنش به تهدیدها استفاده از فناوریهای پیشرفته از جمله یادگیری ماشین و هوش مصنوعی در مرکز عملیات امنیت می باشد که علاوه بر کاهش بار کاری و سرعت بخشیدن به پردازش انبوه رخدادهای دریافت شده از محصولات حفاظتی، از وقوع خطای انسانی نیز پیشگیری می نماید.

چالشهای مهم در برقراری امنیت

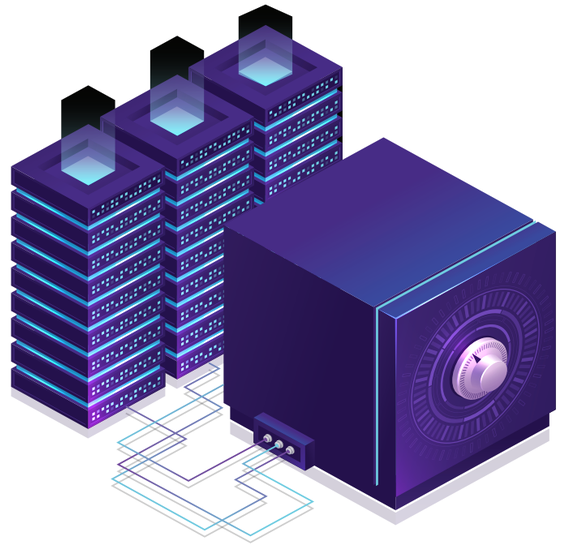
- انبوه هشدارهای امنیتی که بطور مداوم توسط محصولات حفاظتی مخابره می شوند و نیازمند بررسی دقیق در زمان مناسب می باشند.
- تعدد و گوناگونی ابزارهای حفاظتی که برای پوشش دهی نیازهای مختلف بطور همزمان مورد استفاده قرار میگیرند.
- طولانی بودن فرایند تحلیل رخدادها به دلیل وابستگی به اطلاعات و تجربه نیروی متخصص و با در نظر گرفتن ضریب احتمال خطای انسانی.
- در دسترس نبودن منابع لازم برای واکنش در زمان رخداد شامل نیروی انسانی، منابع اطلاعاتی و تجهیزات.

راهکار امنیت جامع علم و صنعت با رفع چالشها و تنگناها و نیز سرعت بخشیدن به عملیات پردازش رخدادها، برقراری امنیت در سراسر شبکه را برای شما تامین می کند.

- ارزیابی امنیت نقاط پایانی، سرورها و سرویسها، زیرساخت مجازی و زیرساخت شبکه
- طراحی ساختار امنیت شبکه بر مبنای استانداردهای معتبر و سیاستهای سازمانی
- نصب و راه اندازی سامانه مدیریت جامع تهدید ها
- پیاده سازی راهکار مدیریت دسترسی به شبکه
- پیاده سازی سامانه مدیریت دسترسی به سرویسها
- راه اندازی سامانه یکپارچه ضدبدافزار
- نصب و راه اندازی سامانه ضدهرزنامه
- برگزاری دوره های آموزشی و آگاه سازی
- ارائه مشاوره و تولید نقشه راه امنیت بر اساس نتایج نیاز ارزیابی های صورت گرفته
- نصب و راه اندازی راهکار مدیریت آسیب پذیری
- پیاده سازی راهکار مدیریت پشتیبانی اطلاعات
- راه اندازی راهکار نصب و گسترش اصلاحیه ها
- مقاوم سازی نقاط پایانی، سرویسها و تجهیزات ارتباطی
- مستند سازی پیکربندی های اعمال شده در محصولات
- بررسی مستمر عملکرد محصولات امنیتی و وضعیت امنیت سایبری
- واکنش و تحلیل رخدادها و خدمات و پشتیبانی نامحدود

راهکار پیشگیری از نشت اطلاعات

خروج و تغییر غیر مجاز اطلاعات از جمله تهدیدهای موثر در افزایش ریسک از دست دادن دارایی های اطلاعاتی محسوب می شوند. عواملی مانند جاسوسی های برنامه ریزی شده با هدف تخریب کسب و کار و یا ایجاد اختلال در چرخه کاری و همچنین ضعفهای طراحی امنیت مانند عدم طبقه بندی اطلاعات و اعمال سیاستهای حفاظتی درون سازمانی، دلایل اصلی خسارتهای ناشی از نشت اطلاعات می باشند.



گامهای مهم درپیشگیری از نشت اطلاعات

- تفکیک اطلاعات بر اساس طبقه بندی های سازمانی
- پایش دسترسی کاربران به داده های حساس
- پایش انتقال داده از طریق وب و ایمیل
- تحلیل رفتارهای سازمانی در زمان تبادل اطلاعات
- اطمینان از امنیت محل قرارگیری اطلاعات
- پایش محتوای فایل های در حال تبادل
- کنترل وسایل ذخیره سازی قابل حمل
- رمزنگاری داده های مهم در زمان انتقال

امکاناتی مانند شناسایی الگوی داده، دسته بندی اطلاعات سازمانی، قواعد پیشگیرانه سازگار با چرخه کاری و نیز تولید هشدار و گزارش‌های کارآمد بمنظور اطلاع از وضعیت تبادل اطلاعات، از جمله عوامل راهبردی در اعمال سیاستهای سازمانی بمنظور پیشگیری از نشت و سرقت اطلاعات می باشند.

روشهای ناامن انتقال داده در شبکه داخلی | دسترسی نفوذگران به منابع اطلاعاتی سازمان | عدم کنترل رفتار و فعالیتهای کارمندان | محل نا امن قرارگیری اطلاعات حساس

جاسوس افزارها و حملات پیشرفته | تبادل ناامن داده در اینترنت و شبکه های خارج سازمان | استفاده از تجهیزات شخصی برای مصارف سازمانی

راهکار پیشگیری از نشت اطلاعات آمیخته ای از فناوری های حفاظتی است که بر اساس سیاستهای امنیتی سازمان، دارایی‌های اطلاعاتی شما را حفظ و از سرقت و یا تغییر غیر مجاز آنها پیشگیری می کند.

- ارائه خدمات مشاوره و طراحی سیاستهای حفاظت از دارایی های اطلاعاتی
- نصب و راه اندازی سامانه مدیریت دسترسی به اینترنت
- مقاوم سازی نقاط پایانی، سرویسها و تجهیزات ارتباطی در برابر تهدید ها
- شناسایی الگوی تبادل داده های سازمانی و اعمال سیایتهای امنیتی مناسب
- ارزیابی امنیت نقاط پایانی، سرورها و سرویسها، زیرساخت مجازی و زیرساخت شبکه
- طراحی و راه اندازی راهکار پیشگیری از نشت اطلاعات
- پیاده سازی سامانه پشتیبانی اطلاعات
- پیاده سازی و راه اندازی راهکار نصب و گسترش اصلاحیه
- مستند سازی پیکربندی های اعمال شده در محصولات
- برگزاری دوره های آموزشی و آگاه سازی

چرا علم و صنعت

گروه امنیت فناوری اطلاعات علم و صنعت با توان و ظرفیتهای ۳۰ ساله این شرکت و به پشتوانه تجربه متخصصان حوزه امنیت فناوری اطلاعات، با هدف ایجاد تحول در روند ارائه راهکارهای نوین حوزه امنیت فناوری اطلاعات، در سال ۱۳۹۸ شروع به فعالیت نمود.

شناسایی نیازمندیهای مشتریان ایرانی و نیز مطالعه و بکارگیری استانداردهای جهانی در ارائه محصولات برتر و خدمات با کیفیت، سرلوحه فعالیت های علم و صنعت می باشد. این شرکت با بهره مندی از گسترده ترین شبکه نمایندگی در سراسر کشور، تجربه استفاده از نسل جدید خدمات و محصولات امنیت فناوری اطلاعات را به مشتریان محترم تقدیم می نماید.

توانمندی ها

وسیع ترین شبکه نمایندگی فروش محصولات و خدمات پس از فروش در کشور

تیم تخصصی طراحی و استقرار راهکارها

بزرگترین گروه پشتیبانی محصولات و خدمات پس از فروش در کشور

ارایه محصولات و راهکارهای نوین شرکتهای برتر بین‌المللی

ویژگی ها

مطالعه و بکارگیری استانداردهای جهانی

بازنگری مداوم سطح کیفیت خدمات

تشخیص صحیح نیازمندیهای مشتریان

تحقیق و توسعه راهکارهای نوین

ارائه راهکارهای سازگار با کسب و کار

تیم فنی متخصص

برنامه ریزی و مدیریت پروژه

خط مشی

افزایش سطح امنیت کسب و کار

ارتقاء سطح آگاهی و دانش مشتریان

پوشش دهی درخواستهای مشتریان ایرانی

جلب اعتماد و حفظ رضایت مشتریان

کسب دانش و شناسایی راهکارهای نوین

افزایش سطح کیفیت خدمات

گسترش خدمات و راهکارها

ارزش سازمانی

حقوق بشر و ارزشهای انسانی

وظیفه شناسی و مسئولیت پذیری

گسترش نیروی انسانی و افزایش انگیزه کاری

مشتری مداری و تامین خواسته های مشتریان

استمرار و پایداری در تداوم کسب و کار

اخلاق و رقابت حرفه ای

خلاقیت و نوآوری

ما در مسیر ارائه بالاترین سطح کیفیت خدمات امنیت فناوری اطلاعات، از توانمندی مجرب ترین نیرو های متخصص بهره گرفته ایم تا با ایجاد تحول، تجربه ای منحصر بفرد از خدمات ویژه را به شما تقدیم کنیم.

شرکت کامپیوتری
علم و صنعت