توصیه نامه امنیتی

دورکار امن کارکنان

شبکه گستر

امنیت شما | وظیفه ما

فهرست مطالب

چکیده مدیریتی

ویروس کووید ۱۹ نخستین بار در آذر ماه در شهر ووهان چین شناسایی شد. در حالی که ابتدا از بیماری ناشی از این ویروس با عنوان ذات‌الریه یاد می‌شد کمیسیون ملی بهداشت چین در دی ماه به‌صورت رسمی شیوع کووید ۱۹ را در این کشور گزارش کرد. یک ماه بعد سازمان بهداشت جهانی شیوع این ویروس را یک همه‌گیری محدود (Outbreak) و تهدیدی برای سلامت عموم در سطح بین‌الملل اعلام کرد. این سازمان در ۲۱ اسفند ۱۳۹۸ خبر داد که کووید ۱۹ به مرحله همه‌گیری جهانی (Epidemic) رسیده است. دبیرکل سازمان ملل انتشار این ویروس را بدترین بحران جهانی از زمان پایان جنگ جهانی دوم در ۷۵ سال گذشته توصیف کرده است.

کشورهای مختلف هر یک با سیاست‌هایی خاص به مقابله با این ویروس پرداخته‌اند. از جمله این سیاست‌ها که در ایران نیز در حال اجراست، فاصله‌گذاری اجتماعی است. از اقدامات مؤثر در ایجاد فاصله‌گذاری اجتماعی انجام دورکاری کارکنان از منزل بجای حضور فیزیکی در محل کار است.

علاوه بر فراهم بودن ارتباط اینترنتی مناسب، انضباط، خودانگیزشی و روالی جامع و مشخص، اطمینان از تأمین امنیت سیستم‌ها و داده‌های ذخیره و تبادل شده از نکات حائز اهمیت در انجام اثربخش و امن دورکاری است.

در این توصیه‌نامه به مواردی که رعایت آنها نقشی کلیدی در ایمن نگاه داشتن سازمان از گزند تهدیدات سایبری در جریان دور کاری دارند پرداخته شده است.

نصب ضـدویـروس؛ امنیـت پـایه دستـگاه‌ها

از امنیت کامپیوتر یا لپ‌تاپ شخصی کارکنان، به خصوص در زمانی که قرار است از طریق آنها اقدام به دورکاری کنند به هیچ عنوان نمی‌توان چشم‌پوشی کرد. اولین قدم اطمینان از نصب بودن ضدویروس بر روی این دستگاه‌هاست. استفاده از ضدویروس مبتنی بر یک سامانه مدیریتی رایانش ابری ضمن حفاظت از دستگاه کاربران، سازمان را در هر لحظه قادر به رصد وضعیت امنیتی دستگاه‌ها در هر کجای جهان که هستند می‌کند. نسخه Cloud راهکار جامع Bitdefender GravityZone نمونه‌ای از محصولات امنیتی مجهز به سامانه ابری است. در این راهکار بدون نیاز به هر گونه سرور مدیریتی می‌توان ضدویروس نصب شده بر روی دستگاه کاربران را در هر نقطه از دنیا به‌صورت متمرکز پیکربندی و مدیریت کرد. محصول نصب شده بر روی سیستم کارکنان، علاوه بر ضدبدافزار، دارای قابلیت‌های دیواره آتش، کنترل و پویش دستگاه‌های ذخیره‌سازی، پالایش محتوای وب، دسته‌بندی نشانی‌های URL و کنترل برنامه‌هاست که جزیی‌ترین اجزای هر یکی از آنها بر اساس سیاست‌های سازمان در کنسول ابری Bitdefender GravityZone قابل پیکربندی است.

بکـارگیری رمـزهای عبـور پیچیـده؛ همیـشه و همـه‌جـا

عدم استفاده از رمزهای عبور پیچیده برای تمامی کاربران به‌خصوص کاربران با سطح دسترسی بالا می‌تواند شبکه و اطلاعات سازمان را در معرض خطر قرار دهد. توجه به نکات زیر لازم و ضروری است:

- عدم استفاده از رمزهای عبور ساده
- پرهیز از استفاده مجدد از رمز عبوری که قبلاً مورد استفاده قرار گرفته است
- استفاده از قابلیت اصالت‌سنجی چندمرحله‌ای در هر کجا که امکان آن فراهم است
- اطمینان از تخصیص رمز عبور منحصربه‌فرد به هر حساب کاربری
- تغییر دوره ای رمزهای عبور

نصب اصلاحیه‌های امنیتی؛ همواره ضروری

دستگاه‌های با سیستم عامل / برنامه حاوی ضعف امنیتی، سازمان را در برابر بسیاری از بدافزارها و حملاتی همچون نصب از راه دور کد مخرب، سرقت داده‌ها و از کاراندازی سرویس (DoS) آسیب‌پذیر می‌کنند. وجود یک ضعف امنیتی در سیستم عامل یا هر یک از برنامه‌های نصب شده بر روی دستگاه می‌تواند سبب دور زدن قوی‌ترین نرم‌افزارهای ضدویروس یا دیواره‌های آتش شود. لذا نصب به‌موقع بسته‌ها و اصلاحیه‌های امنیتی بر روی تمامی دستگاه‌ها از جمله سیستم‌های مورد استفاده توسط کارکنان در جریان دور کاری توصیه اکید می‌شود.

برای آن دسته از سازمان‌هایی که مایلند که نصب، به‌صورت متمرکز و طبق روالی مشخص بر روی سیستم کاربران دور کار انجام شود استفاده از Patch Management در راهکار Bitdefender GravityZone را پیشنهاد می‌کنیم. این محصول سازمان را قادر می‌سازد تا سیستم‌های عامل Windows و نرم‌افزارهای مبتنی بر این سیستم عامل را بر روی دستگاه‌ها به‌صورت متمرکز مجهز به آخرین اصلاحیه‌ها و به‌روزرسانی‌ها نماید.

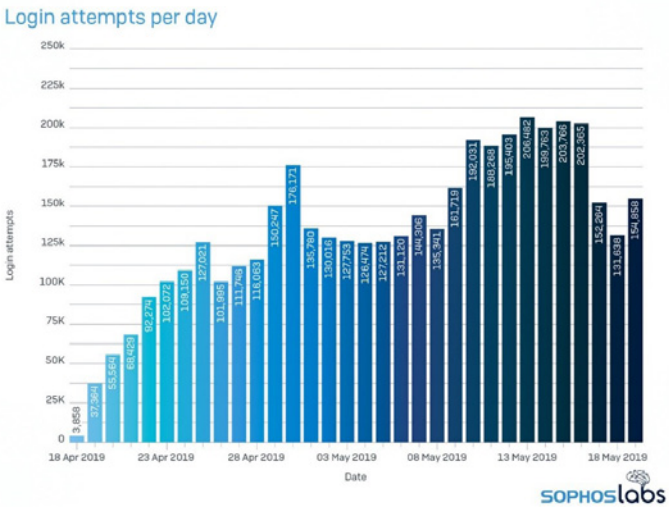
استفـاده از رمزگـذاری؛ تا حـد امکـان

لپ‌تاپ‌های حاوی اطلاعات حساس و محرمانه که توسط کارکنان از سازمان خارج می‌شوند همواره در خطر مفقود یا سرقت شدن قرار دارند. هر چند ممکن است جایگزین نمودن یک لپ‌تاپ، هزینه قابل توجه‌ای را متوجه سازمان نکند اما نشت و درز اطلاعات سـازمان را با عواقبی بعضاً جبران‌ناپذیر مواجه می‌کند.

محصولاتی همچون Bitdefender Full Disk Encryption و McAfee Drive Encryption با رمزگذاری کل دیسک، این اطمینان را فراهم می‌سازند که در صورت مفقود یا سرقت شدن دستگاه، داده‌های ذخیره شده بر روی آن از دید افراد غیرمجاز پنهان و غیرقابل دسترس باقی بماند. نرم‌افزار McAfee File and Removable Media Protection نیز بر اساس سیاست‌های سازمان، رمزنگاری خودکار و نامحسوس اطلاعات را در محیط‌ها و بسترهای مختلف ممکن می‌کند. این نرم‌افزار امکان رمزنگاری فایل‌ها و پوشه‌های ذخیره شده یا به اشتراک گذاشته شده بر روی کامپیوترها، سرورهای فایل، ایستگاه‌های کاری VDI، پیوست‌های ایمیل، حافظه‌های جداشدنی - نظیر USB Flash -، فایل‌های ISO، سیستم‌های Mac و سرویس‌های ذخیره‌سازی ابری را به‌صورت خودکار، نامحسوس و بر اساس پیکربندی متمرکز فراهم می‌کند. بنابراین حتی در صورت خروج این اطلاعات به دلیل رمزگذاری شدن آنها، افراد غیرمجاز قادر به خواندن آنها نخواهند بود.

مقـاوم‌سـازی RDP؛ پودمـان مورد علاقـه مهـاجمان

در سال‌های اخیر سوءاستفاده از پودمان Remote Desktop Protocol - به اختصار RDP - توسط مهاجمان سایبری افزایش چشمگیری داشته است. علاوه بر مدیران شبکه که از این پودمان برای اتصال به سرورها و ایستگاه‌های کاری سازمان استفاده می‌کنند، در بسیاری از سازمان‌های کوچک و متوسط نیز از RDP برای برقرار نمودن ارتباط از راه دور پیمانکاران حوزه فناوری اطلاعات، به سرورهایی همچون حقوق و دستمزد، اتوماسیون اداری و غیره استفاده می‌شود. دورکاری نیز عاملی در استفاده هر چه بیشتر از این پودمان خواهد بود. واقعیت آن است که میلیون‌ها دستگاه با RDP قابل دسترس در بستر اینترنت نقشی اساسی در گسترش آلودگی‌ها در سطح جهان دارند. تصویر زیر تعداد تلاش مهاجمان برای ثبت ورود (Login) به دستگاه‌های با RDP باز را که شرکت سوفوس آنها را به‌عنوان Honeypot راه‌اندازی کرده است در بازه‌ای یک‌ماهه نشان می‌دهد.



مهاجمان از ابزارهایی نظیر Shodan برای شناسایی سرورهای با پودمان RDP قابل دسترس بر روی اینترنت استفاده کرده و در ادامه با بکارگیری ابزارهایی همچون NLBrute اقدام به اجرای حملات موسوم به "سعی‌وخطا" (Brute Force) می‌کنند.

هدف از اجرای حملات "سعی‌وخطا" رخنه به دستگاه از طریق پودمانی خاص - در اینجا RDP - با بکارگیری ترکیبی از نام‌های کاربری و رمزهای عبور رایج است. بنابراین در صورتی که دسترسی به پودمان RDP از طریق کاربری با رمز عبور ساده و غیرپیچیده باز شده باشد مهاجمان نیز به‌راحتی امکان اتصال به دستگاه را خواهند داشت. در ادامه هم با استفاده از ابزارهایی همچون Mimikatz قادر به استخراج اطلاعات اصالت‌سنجی حساب‌های کاربری با سطح دسترسی بالا همچون حساب‌های Domain Admin و نفوذ به سایر سیستم‌ها خواهند بود.

متأسفانه در اکثر مواقع این سرورها هستند که پودمان RDP آنها در بستر اینترنت قابل دسترس است. سرورها بنا به ماهیت و عملکردشان عمدتاً حاوی اطلاعاتی بسیار حساس، با ارزش‌های مالی و معنوی بالا هستند. به‌همین خاطر در صورت موفقیت در رخنه به آنها منافع قابل‌توجهی متوجه مهاجمان خواهد شد.

در برخی موارد نیز مهاجمان با انتخاب دقیق اهداف خود، پس از نفوذ به یکی از سرورهای با دسترسی RDP باز، اقدام به اجرای عملیات شناسایی (Reconnaissance) بر ضد کارکنانی خاص کرده و پس از استخراج اطلاعات مورد نیاز، آنها را با فیشینگ‌های هدفمند (Spear Phishing) مورد حمله قرار می‌دهند تا از این طریق به داده‌های حساس سازمانی نظیر اطلاعات اصالت‌سنجی لازم برای ورود به سامانه‌ها دست پیدا کنند.

به تمامی مدیران و راهبران شبکه‌ها در هر اندازه‌ای توصیه می‌شود تحت هیچ شرایطی، حتی برای مدتی کوتاه دسترسی به شبکه سازمان را از طریق سازوکار RDP بدون در نظر داشتن توصیه‌ها و الزامات امنیتی فراهم نکنند.

حفـاظت از دادهـا؛ حسـاس‌تـر از قبـل

داده‌ها بااهمیت‌ترین دارایی در اقتصاد دیجیتال محسوب می‌شوند. در صورت انتقال اطلاعات بر روی سیستم های شخصی، حفاظت از آنها بیش از هر زمانی دیگر اهمیت پیدا می‌کند. فرایند جلوگیری از خروج اطلاعات بر روی سیستم‌ها با کنترل فراگیر داده‌ها حتی پس از اعمال شدن تغییر بر روی آنها آغاز می‌شود.

سازمان باید از طریق محصولات مناسب نحوه انتقال داده‌های حساس از طریق رسانه‌های مختلف همچون ایمیل، پیام‌رسان‌های فوری، چاپگرها، حافظه‌های جانبی و بسیاری موارد دیگر را قانونمند کند. اهمیتی ندارد که داده‌ها در سازمان باشند، در منزل باشند یا در حال حرکت باشند؛ هر کجا که هستند سیاست‌ها و قواعد تعریف شده بر روی آنها باید اعمال شود.

برای مثال در نرم‌افزار McAfee Data Loss Prevention می‌توان جزئی‌ترین ویژگی‌های یک فایل را تعریف کرد تا نرم‌افزار نسبت به استفاده غیرمجاز از آن فایل واکنش نشان دهد. این نرم‌افزار امکان نظارت و کنترل بر روی انتقال اطلاعات از کامپیوتر کاربران را فراهم می‌کند؛ حتی اگر کامپیوترها به شبکه سازمانی متصل نباشند. این سازمان است که تعیین می‌کند چه وسایلی قابل استفاده و چه وسایلی غیرقابل استفاده برای کپی و انتقال اطلاعات هستند. همچنین تعیین اطلاعات قابل کپی و انتقال به وسایل مجاز نیز از طریق این نرم‌افزار قابل تعریف است. به‌طور خلاصه McAfee Data Loss Prevention قادر به مسدودسازی و کنترل راه‌های خروج اطلاعات از جمله موارد زیر می‌باشد:

- وسایل ذخیره‌سازی قابل حمل نظیر USB Flash و DVD/CD
- ارتباطات بی‌سیم همچون IrDA، Bluetooth و Wi-Fi
- درگاه های فیزیکی موجود بر روی دستگاه نظیر COM، USB، Firewire 1394 و LPT1
- ارسال اسناد با استفاده از پودمان‌هایی همچون HTTPS، FTP و HTTP
- نرم‌افزارهایی که به داده‌ها دسترسی می‌یابند؛ نظیر مرورگرها، برنامه‌های مدیریت ایمیل، برنامه‌های فشرده‌ساز و پیام‌رسان‌ها
- چاپگرهای متصل به کامپیوتر، چاپگرهای اشتراکی در شبکه و چاپگرهای PDF و تصویری
- حافظه موقت (Clipboard)
- سرویس‌دهندگان رایانش ابری نظیر Syncplicity، SkyDrive، Dropbox، Google Drive و Box
- تصویربرداری از پنجره ها از طریق کلید Print Screen و نرم افزارهای استفاده کننده از Graphics Device Interface

پویـش ایمیـل‌ها؛ پیـش از رسیـدن به دستـگاه کـاربر

کرود استرایک گزارش کرده که حملات فیشینگ هدفمند با هدف رخنه اولیه به یک شبکه در ۳۵ درصد از کیس‌های مورد بررسی توسط این شرکت در سال ۲۰۱۹ نقش داشته است که در مقایسه با سال قبل از آن ۲ درصد رشد را نشان می دهد. ایمیل هایی که با لینک / پیوست مخرب و با بهره گیری از ترفندهای مهندسی اجتماعی اقدام به سرقت اطلاعات حساسی همچون نام کاربری و رمز عبور می کنند. دور کاری می‌تواند عاملی برای افزایش تبادل ایمیل میان کارکنان شود. با توجه به قابل دسترس شدن شبکه سازمان از روی دستگاه کارمند، موفقیت مهاجم در رخنه به دستگاه می‌تواند تهدیدی جدی باشد. علاوه بر آموزش کاربران و آگاهی‌رسانی به آنها در خصوص تهدیدات مبتنی بر ایمیل بهره‌گیری از محصولات ویژه حفاظت از سرویس‌دهندگان ایمیل همچون McAfee Security for Email Servers، Bitdefender GravityZone Enterprise Security for Exchange و Sophos Email Protection با قابلیت‌هایی همچون ضدبدافزار، ضدهرزنامه و ضدفیشینگ اهمیت بسزایی دارد.

دیواره آتش؛ الزامی برای سرویس‌های قابل دسترس بر روی اینترنت

سوءاستفاده مهاجمان از سرویس‌های قابل دسترس در بستر اینترنت به‌منظور رخنه به شبکه سازمان محدود به RDP نمی‌شود. در سال‌های اخیر، دامنه گسترده‌ای از این پودمان‌ها مورد توجه نفوذگران و گردانندگان بدافزار قرار گرفته است. به‌طور ویژه سرورهای Microsoft SQL در معرض حملات گسترده‌ای قرار دارند. برای مثال می‌توان به بدافزار پیشرفته Lemon_Duck اشاره کرد که در سال ۱۳۹۸ مهاجمان با بکارگیری آن اقدام به اجرای حملات رمز ربایی (Cryptojacking) بر ضد سازمان‌ها در بسیاری از کشورها از جمله ایران کردند. در جریان حملات این مهاجمان، فهرستی از نشانی‌های IP به‌صورت تصادفی ایجاد شده و پس از مورد هدف قرار دادن آنها، قابل دسترس بودن چندین درگاه از جمله TCP/۱۴۳۳ که درگاه پیش‌فرض MS-SQL است مورد بررسی قرار می‌گیرد. چنانچه درگاه ۱۴۳۳ بر روی دستگاه هدف باز باشد بدافزار اقدام به اجرای حملات موسوم به "سعی‌وخطا" (Brute-force) جهت رخنه به سرویس‌دهنده MS-SQL نصب‌شده بر روی دستگاه می‌کند. برای این منظور Lemon_Duck با بکارگیری رمزهای عبور رایج و مجموعه‌ای از هش NTLM تلاش می‌کند تا حساب کاربری sa در سرویس Microsoft SQL را هک کند. به‌محض موفقیت در هک حساب کاربری مذکور، بدافزار با استفاده از پروسه sqlserver.exe فرامین مخرب را بر ضد ماشین‌های دیگر اجرا می‌کند. یک جستجوی ساده در سایت BinaryEdge نشان می‌دهد که در حال حاضر حدود ۲۱ هزار سرویس‌دهنده SQL مستقر در شبکه سازمان های ایرانی با درگاه پیش‌فرض ۱۴۳۳ بر روی اینترنت قابل دسترس هستند. یا در نمونه‌ای دیگر می توان از باج‌افزارهایی نام برد که با نفوذ به دستگاه‌های ذخیره‌ساز متصل به شبکه که در بستر اینترنت به طریقی غیرامن در دسترس قرار گرفته‌اند، اقدام به رمزگذاری فایل‌های ذخیره شده بر روی آنها کرده و در ازای آنچه که بازگرداندن فایل‌ها به حالت اولیه می‌خوانند، مبلغی را از قربانی اخاذی می‌کنند.

علاوه بر مقاوم‌سازی سرویس‌های مورد استفاده توسط سازمان به ویژه سرویس‌های قابل دسترس بر روی اینترنت، بکارگیری تجهیزات پیشرفته دیواره آتش و مدیریت تهدید یکپارچه (UTM) همچون Sophos XG Firewall برای حفاظت از آنها از گزند دسترسی غیرمجاز توصیه اکید می‌شود.

امـن‌سـازی ارتبـاطات؛ مهـم‌تر از قبـل

برای دورکاری لازم می‌شود که دسترسی کاربران به سرویس‌ها و برنامه‌های کاربردی درون سازمان از طریق اینترنت فراهم شود. این موضوع می‌تواند مخاطرات زیادی را برای حفظ محرمانگی اطلاعات سازمان که در بستر اینترنت جابجا می‌شوند ایجاد کند. هنوز هم هستند بسیاری از برنامه‌های کاربردی که اطلاعات خصوصی افراد و سازمان مانند رمز کاربران را به‌صورت رمز نشده در شبکه منتقل می‌کنند. موضوعی که وقتی اطلاعات در شبکه جهانی اینترنت جابجا می‌شود می‌تواند مشکلات امنیتی زیادی را ایجاد کند.

لازم است که در راه‌حل‌های دورکاری موضوع رمزگذاری اطلاعات سازمانی، در زمان جابجایی در اینترنت بطور جدی مدنظر باشند. در حال حاضر بهترین راه‌حل برای رمزگذاری اطلاعات در زمان انتقال در شبکه‌ها، استفاده از پودمان‌های VPN می‌باشد.

استفاده از پودمان Virtual Private Network - به اختصار VPN - این اطمینان را فراهم می‌کند که تمامی داده‌های تبادل شده در بستر شبکه جهانی اینترنت میان دستگاه کارمند و شبکه سازمان رمزگذاری شده و از گزند افراد غیرمجاز در امان باشد. برای این منظور می‌توانید از امکانات متنوع Sophos XG Firewall بهره بگیرید.

کنتـرل دستـرسی کاربـران به اینتـرنت

فعالسازی پالایش وب بر روی دستگاه‌های کاربران توصیه می‌شود. با این کار هم از دسترسی کاربران به سایت‌های غیرکاری در زمان دورکاری جلوگیری می‌شود و هم امنیت داده‌های کاربران و سازمان در برابر تهدیدات اینترنتی از جمله بدافزارها کنترل می‌شود. قابلیت‌های متنوع Web Protection در دیواره‌های آتش Sophos به‌سادگی این امکان را فراهم می‌کنند.

انجام نظارت و پایش؛ مستمر و پویا

راهبران باید به‌طور مستمر با بهره‌گیری از نرم‌افزارها و سامانه‌های مناسب، ارتباطات، وضعیت به‌روزرسانی و نصب محصولات و وقایعی همچون رخدادهای مرتبط با بدافزارها و یا نشت اطلاعات را مورد رصد و کنترل قرار دهند. کارکنان نیز می‌بایست از نحوه اطلاع‌رسانی به افراد مربوطه در زمان مواجهه با موارد مشکوک یا بروز رخدادهای امنیتی بر روی دستگاه مورد استفاده خود آگاه باشند. فراموش نکنیم که دور کاری به‌معنای گسترده‌تر شدن دامنه شبکه سازمان و در معرض قرار گرفتن آن در بستر شبکه جهانی اینترنت بوده و تأمین امنیت آن مستلزم واکنش به‌موقع به کلیه رویدادهای مرتبط با آن است.

آخـرین اخبـار امنیـت فنـاوری اطلاعات

@SGnewsroom

شبکه گستر

شرکت مهندسی شبکه گستر در سال ۱۳۷۰ تأسیس گردید و اولین شرکت ایرانی است که در زمینه نرم‌افزارهای ضدویروس فعالیت تخصصی و متمرکزی را آغاز کرده است. در ابتدا، همکاری مشترکی بین شرکت مهندسی شبکه گستر و شرکت انگلیسی S & S International (تولیدکننده ضدویروس مشهور Toolkit) آغاز گردید. در مدت کوتاهی، با فعالیت شبکه گستر به عنوان نماینده رسمی و انحصاری S & S International در ایران، به تدریج ضدویروس Dr Solomon's Toolkit به محبوب‌ترین ضدویروس در ایران تبدیل شد. پس از خرید شرکت S & S International توسط شرکت McAfee در سال ۱۳۷۷، شرکت شبکه گستر نیز مانند دیگر نمایندگان بین‌المللی فعالیت خود را بر روی نرم‌افزارهای ضدویروس McAfee ادامه داد. اکنون نیز شبکه گستر به عنوان فروشنده مجاز (Authorized Reseller) در منطقه خاورمیانه، به ارائه محصولات و خدمات در ایران اقدام می‌نماید. در سال ۱۳۸۴ شرکت مهندسی شبکه گستر موفق به کسب نمایندگی رسمی شرکت آلمانی Astaro، سازنده محصولات مدیریت یکپارچه تهدیدات (Unified Threat Management) گردید. به دنبال رشد چشمگیر و موفقیت جهانی محصولات امنیتی شرکت Astaro، در سال ۱۳۹۰ شرکت Sophos انگلیس، اقدام به خرید این شرکت آلمانی نمود. به دنبال این نقل و انتقال، شرکت مهندسی شبکه گستر با همکاری با شرکت Sophos، فعالیت خود را در این زمینه ادامه داده و اکنون محصولات Astaro سابق را تحت نام Sophos در ایران عرضه می‌نماید. از سال ۱۳۹۱ شرکت مهندسی شبکه گستر عرضه محصولات ضدویروس Bitdefender را به عنوان نماینده و توزیع‌کننده (Distributor) رسمی در ایران آغاز کرد. عرضه محصولات ضدویروس Bitdefender در کنار محصولات امنیتی McAfee، پاسخی به شرایط و نیازهای متفاوت کاربران و مدیران شبکه بوده است. ضدویروس چابک‌تر، مدیریت آسان‌تر و محصولی مقرون به صرفه‌تر، انتظارات برخی از کاربران و مدیران شبکه بود که با عرضه محصولات ضدویروس Bitdefender، شبکه گستر به نیازهای این بخش از بازار پاسخ داد. شرکت مهندسی شبکه گستر افتخار دارد که مجری برخی از بزرگترین پروژه‌های نصب و راه‌اندازی و طولانی مدت‌ترین قراردادهای نگهداری و پشتیبانی محصولات امنیت شبکه در کشور بوده است. این شرکت علاوه بر خدمات‌دهی به هزاران شرکت و سازمان که صدها هزار کاربر را در کشور شامل می‌شوند، دارای شبکه نمایندگی فروش و پشتیبانی در سراسر کشور نیز می‌باشد.

شرکت مهندسی شبکه گستر

تهران ۱۹۶۸۶، خیابان شهید دستگردی (ظفر)، شماره ۲۷۳

تلفن / دورنگار	۰۲۱-۴۲۰۵۲
رایانامه	info@shabakeh.net
تارنمای شرکت	www.shabakeh.net
خدمات پس از فروش و پشتیبانی	my.shabakeh.net
مرکز آموزش	events.shabakeh.net
اتاق خبر	newsroom.shabakeh.net