وزارت ارتباطات و فناوری اطلاعات
سازمان فناوری اطلاعات ایران

مرکز ماهر

الزامات امنیتی سایبری و فیزیکی دورکاری

کارکنان دستگاه‌های دولتی

فهرست مطالب

۱- مقدمه

با توجه به شرایط بوجود آمده در جهان و متعاقبا در کشور ناشی از همه‌گیری بیماری Covid-۱۹ و لزوم به حداقل رساندن حضور پرسنل و کارشناسان در محل کار و الزام به انجام فعالیت ها بصورت دورکاری، ذکر چند نکته امنیتی برای کاهش ریسک و خطرات ناشی از ارتباطات از راه دور ضروری می‌باشد. دورکاری یا کار از راه دور به کارمندان یک سازمان، پیمانکاران، شرکای تجاری، فروشندگان و سایر کاربران این امکان را می‌دهد که کار خود را از مکان‌هایی غیر از مکان سازمان انجام دهند. دورکارها از ابزارهای مختلفی مانند رایانه‌های رومیزی و لپ‌تاپ‌ها، تلفن‌های هوشمند و تبلت‌ها برای خواندن و ارسال ایمیل، دسترسی به وبگاه‌ها، بررسی و ویرایش اسناد و کارهای دیگر استفاده می‌کنند. دستگاه‌های دورکارها ممکن است توسط سازمان، توسط اشخاص ثالث (پیمانکاران سازمان، شرکای تجاری یا فروشندگان) یا توسط خود کاربران کنترل شوند. اکثر کارمندان دورکار این امکان را دارند که به منابع محاسباتی غیرعمومی سازمان از مکان‌های خارجی، غیر از مکان سازمان، دسترسی داشته باشند.

دورکاری و راه‌کارهای دسترسی از راه دور به‌طور معمول نیاز به پشتیبانی از چندین هدف امنیتی دارند. این موارد از طریق ترکیبی از ویژگی‌های امنیتی که در راه‌کارهای دسترسی از راه دور قرار داده می‌شود و کنترل‌های امنیتی اضافه‌ای که به دستگاه‌های کارمندان دورکار اعمال می‌شود و دیگر مؤلفه‌های راه‌کار دسترسی از راه دور، انجام می‌شود. متداول‌ترین اهداف امنیتی فناوری‌های دورکاری و دسترسی از راه دور شامل اطمینان از غیر قابل خوانده شدن داده‌های ذخیره‌شده‌ی کاربر توسط بخش‌های غیرمجاز در ارتباطات با دسترسی از راه دور (محرمانگی)، تشخیص هرگونه تغییر عمدی یا غیرعمدی در ارتباطات دسترسی از راه دور و اطمینان دسترسی به منابع به کاربران از طریق دسترسی از راه دور است

برای دستیابی به این اهداف، تمام مؤلفه‌های دورکاری و راه‌کارهای دسترسی از راه دور، از جمله دستگاه‌های کارمندان دورکار، سرویس‌دهنده‌های دسترسی از راه دور و سرویس‌دهنده‌های داخلی که از طریق دسترسی از راه دور مورد دسترسی قرار می‌گیرند، باید در برابر انواع تهدیدات امن‌سازی شوند.

فناوری‌های دورکاری و دسترسی از راه دور اغلب به حفاظت اضافی احتیاج دارند زیرا طبیعت آن‌ها باعث می‌شود که، در مقایسه با فناوری‌هایی که فقط از داخل سازمان در دسترس هستند، در معرض افشای بالاتری نسبت به

تهدیدهای بیرونی قرار داشته باشند. سازمان‌ها قبل از طراحی و به‌کارگیری دورکاری و راه‌کارهای دسترسی از راه دور، باید مدل‌های تهدیدات سیستم را برای سرویس‌دهنده‌های دسترسی از راه دور و منابعی که از طریق دسترسی از راه دور در دسترس هستند، تهیه کنند. مدل‌سازی تهدید شامل شناسایی منابع مورد علاقه و تهدیدات عملی، آسیب‌پذیری‌ها و کنترل‌های امنیتی مرتبط با این منابع است. سپس احتمال حملات موفقیت‌آمیز و تأثیرات آن‌ها را کمی‌سازی کرده و درنهایت این اطلاعات را تجزیه و تحلیل کرده تا تعیین کنند که چه کنترل‌های امنیتی باید بهبود یافته یا اضافه شوند. مدل‌سازی تهدید به سازمان‌ها کمک می‌کند تا الزامات امنیتی را شناسایی کرده و راه‌کارهای دسترسی از راه دور را به‌گونه‌ای طراحی کنند تا کنترل‌های لازم برای برآورده‌کردن الزامات امنیتی را در خود بگنجانند. نگرانی‌های عمده امنیتی در مورد این فناوری‌ها که در اکثر مدل های تهدید دورکاری گنجانده شده است به شرح زیر است:

- فقدان کنترل‌های امنیتی فیزیکی. دستگاه‌های سرویس‌گیرنده دورکاری در مکان‌های مختلف خارج از کنترل سازمان مانند خانه کاربران، کافی‌شاپ‌ها، هتل‌ها و کنفرانس‌ها استفاده می‌شوند. ماهیت موبایل این دستگاه‌ها احتمال گم یا دزدیده شده آن‌ها را بیشتر می‌کند، و این باعث می‌شود که داده‌های دستگاه‌ها در معرض خطر قرار گیرند. راه‌کارهای اصلی کاهش خسارات امنیتی ناشی از گم شدن یا سرقت دستگاه، رمزنگاری حافظه دستگاه شخص دورکار یا فقط داده‌های حساس روی آن، به‌منظور جلوگیری از بازیابی توسط افراد غیرمجاز، یا ذخیره نکردن اطلاعات حساس در دستگاه‌های مشتری است.
- شبکه‌های ناامن. تقریباً همه دسترسی‌های از راه دور از طریق اینترنت اتفاق می‌افتد، و معمولاً سازمان‌ها هیچ کنترلی بر امنیت شبکه‌های خارجی که توسط مشتریان دورکاری استفاده می‌شوند ندارند. سیستم‌های ارتباطی مورد استفاده برای دسترسی از راه دور شامل شبکه‌های پهن‌باند مانند کابل، و سازوکارهای بی‌سیم مانند IEEE ۸۰۲,۱۱ و شبکه‌های سلولی هستند. این سیستم‌های ارتباطی مستعد استراق‌سمع هستند، که اطلاعات حساس منتقل‌شده در هنگام دسترسی از راه دور را در معرض خطر قرار می‌دهند. حملات مردی در میانه (MITM[۱]) نیز ممکن است برای شنود و تغییر ارتباطات انجام شود.
- دستگاه‌های آلوده در شبکه‌های داخلی. دستگاه‌های کارمند دورکار، اغلب در شبکه‌های خارجی استفاده می‌شوند و سپس به سازمان آورده می‌شوند و مستقیماً به شبکه‌های داخلی سازمان وصل می‌شوند. یک

[۱] Man-In-The-Middle

مهاجم با دسترسی فیزیکی به دستگاه مشتری ممکن است بدافزاری را بر روی دستگاه نصب کند تا داده‌ها را از آن دستگاه و شبکه‌ها و سیستم‌هایی که به آن متصل می‌شوند جمع‌آوری کند. اگر دستگاه مشتری به بدافزار آلوده شده باشد، ممکن است به محض اتصال دستگاه مشتری به شبکه داخلی، این بدافزار در سراسر سازمان گسترش یابد. سازمان‌ها باید فرض کنند دستگاه‌های کارمندان آلوده می‌شوند و کنترل‌های امنیتی خود را بر این اساس برنامه‌ریزی کنند.

- دسترسی خارجی به منابع داخلی. دسترسی از راه دور امکان دسترسی به منابع داخلی مانند سرویس‌دهندها را در اختیار میزبانان خارجی قرار می‌دهد. اگر این منابع داخلی قبلاً از طریق شبکه‌های خارجی قابل دسترسی نبودند، دسترسی به آن‌ها از راه دور، آن‌ها را در معرض تهدیدهای جدید، به‌ویژه از دستگاه‌ها و شبکه‌های غیرقابل اعتماد کارمند قرار می‌دهد و احتمال به خطر افتادن آن‌ها را به میزان قابل توجهی افزایش می‌دهد. هر نوع دسترسی از راه دور که بتواند برای دستیابی به یک منبع داخلی مورد استفاده قرار گیرد، ریسک به خطر افتادن آن منبع را افزایش می‌دهد.

۲- دسترسی‌های کارمندان دورکار

روش‌های دسترسی که بیشتر توسط کارمندان دورکار مورد استفاده قرار می‌گیرد، بر اساس معماری سطح بالای آن‌ها به چهار دسته تقسیم می‌شوند: تونل‌زنی[۲]، درگاه‌ها[۳]، دسترسی دسکتاپ از راه دور[۴] و دسترسی مستقیم به برنامه[۵].

۲-۱- تونل‌زنی

بسیاری از روش‌های دسترسی از راه دور یک تونل ارتباطی امن را ارائه می‌دهند که از طریق آن می‌توان اطلاعات را بین شبکه‌ها از جمله شبکه‌های عمومی مانند اینترنت انتقال داد. تونل‌زنی عبارت است از ایجاد یک تونل ارتباطی امن بین دستگاه کارمند دورکار و سرویس‌دهنده دسترسی از راه دور. تونل‌ها معمولاً از طریق فناوری‌های شبکه خصوصی

[۲] Tunneling
[۳] Portals
[۴] Remote Desktop Access
[۵] Direct Application Access

مجازی (VPN[۶]) ایجاد می‌شوند. هنگامی که یک تونل VPN بین دستگاه کارمند دورکار و دروازه VPN سازمان ایجاد شد، کارمند دورکار می‌تواند از طریق تونل به بسیاری از منابع محاسباتی سازمان دسترسی پیدا کند. برای استفاده از VPN کاربران یا باید از نرم‌افزار VPN مناسب در دستگاه‌های خود برخوردار باشند یا در شبکه‌ای باشند که یک سیستم دروازه VPN روی آن باشد.

۲-۲- درگاه‌ها

دسته دیگر از راه‌کارهای دسترسی از راه دور شامل درگاه‌ها است که دسترسی به یک یا چند برنامه را از طریق یک رابط واحد متمرکز ارائه می‌دهد. دورکار برای دسترسی به درگاه از یک سرویس‌گیرنده درگاه در دستگاه دورکاری خود استفاده می‌کند. بیشتر درگاه‌ها مبتنی بر وب هستند و برای آن‌ها سرویس‌گیرنده درگاه یک مرورگر وب معمولی است. نرم‌افزار مشتری برنامه بر روی سرویس‌دهنده درگاه نصب شده است و با نرم‌افزار سرویس‌دهنده برنامه در سرویس‌دهنده‌های درون سازمان ارتباط برقرار می‌کند. درگاه از ارتباطات بین دستگاه‌های مشتری و درگاه محافظت می‌کند. درگاه‌ها همچنین می‌توانند کاربران را احراز اصالت کرده و دسترسی به منابع داخلی سازمان را محدود نمایند. امروزه معماری بیشتر درگاه‌ها SSL VPN است و در واقع ، بیشتر SSL VPN ها درگاه هستند نه تونل.

راه‌کارهای درگاه که معمولاً برای دسترسی از راه دور استفاده می‌شود محدود به چند نوع هستند. درگاه مبتنی بر وب امکان دسترسی به چندین برنامه مبتنی بر وب را از طریق یک وبگاه درگاه برای کاربر به‌وجود می‌آورد. درگاه SSL VPN یک شکل معمول از درگاه مبتنی بر وب است. نوع دیگر راه‌کارهای درگاه دسترسی به سرویس‌دهنده ترمینال است که به هر دورکار امکان دسترسی به دسکتاپ مجازی استانداردشده‌ی مجزا را می‌دهد. سرویس‌دهنده ترمینال یک سیستم عامل دسکتاپ را شبیه‌سازی کرده و دسترسی به برنامه‌ها را فراهم می‌کند. دسترسی به سرویس‌دهنده ترمینال مستلزم این است که کارمند دورکار یک برنامه ویژه سرویس‌دهنده ترمینال را بر روی دستگاه مشتری نصب کند یا از یک رابط مبتنی بر وب استفاده نماید. یک روش مشابه دیگر دسترسی از راه دور، زیرساخت دسکتاپ مجازی (VDI[۷]) نام دارد که کاربر را به یک سیستم متصل می‌کند که حاوی تصاویر مجازی سیستم‌های عامل و دسکتاپ‌های استاندارد

[۶] Virtual Private Network
[۷] Virtual Desktop Infrastructure

و غیرشبیه‌سازی‌شده است. در این روش وقتی کار دورکار با یک نشست دسترسی از راه دور به پایان رسید، تصویر مجازی از بین می‌رود تا کاربر بعدی دسکتاپ مجازی تمیزی و جدیدی داشته باشد.

۲-۳- دسکتاپ از راه دور

راه‌کار دسترسی دسکتاپ از راه دور امکان کنترل از راه دور یک رایانه رومیزی خاص در سازمان را برای یک دورکار به‌وجود می‌آورد. دورکار کنترل‌های ورودی (به‌عنوان مثال، صفحه کلید، ماوس) را از طریق رایانه از راه دور در اختیار دارد و صفحه نمایش رایانه سازمان را در صفحه دستگاه دورکاری خود مشاهده می‌کند. دسترسی دسکتاپ از راه دور به کاربر این امکان را می‌دهد تا به تمام برنامه‌ها، داده‌ها و منابع دیگری که در رایانه موجود در سازمان وجود دارد، دسترسی پیدا کند.

دو روش اصلی برای دسترسی به دسکتاپ از راه دور وجود دارد: روش مستقیم بین کارمند دورکار و ایستگاه کاری داخلی و روش غیرمستقیم از طریق یک سیستم واسطه قابل اعتماد. با این حال، دسترسی مستقیم اغلب امکان‌پذیر نیست زیرا توسط اغلب دیواره‌های آتش از آن جلوگیری می‌شود. دسترسی غیرمستقیم دسکتاپ از راه دور از طریق یک سرویس‌دهنده میانی انجام می‌شود. این سرویس‌دهنده بعضی اوقات بخشی از دیواره آتش سازمان است، اما بیشتر اوقات توسط یک سرویس تجاری قابل اعتماد یا شخص ثالث در خارج از محیط شبکه سازمان اجرا می‌شود. امنیت این سرویس‌دهنده واسط بسیار مهم است، زیرا وظیفه احراز اصالت صحیح کارمندان دورکار و جلوگیری از دسترسی ترافیک رمزنشده توسط بخش‌های غیرمجاز را بر عهده دارد. همچنین، اگر سیاست امنیتی سازمان نیاز به انواع خاصی از احراز اصالت داشته باشد (مانند احراز اصالت دو عاملی)، سرویس‌دهنده میانی باید از هر دو جهت این نوع احراز اصالت را پشتیبانی کند. نرم‌افزار دسترسی دسکتاپ از راه دور از محرمانگی و یکپارچگی ارتباطات دسترسی از راه دور محافظت می‌کند و همچنین کاربر را احراز اصالت می‌کند تا اطمینان حاصل شود که فرد دیگری به ایستگاه کاری داخلی وصل نمی‌شود. با این حال، از آن‌جایی‌که این شامل رمزنگاری انتها به انتهای ارتباطات در سراسر محیط سازمان است، محتویات ارتباطات از کنترل‌های امنیتی شبکه در محیط سازمان، مانند دیواره‌های آتش و سیستم‌های تشخیص نفوذ، پنهان می‌شوند.

۲-۴- دسترسی مستقیم به برنامه

با دسترسی مستقیم به برنامه، دسترسی از راه دور بدون استفاده از یک نرم‌افزار برای دسترسی از راه دور انجام می‌شود و یک دورکار می‌تواند مستقیماً به یک برنامه خاص دسترسی پیدا کند و خود برنامه مسئول تأمین امنیت خود است. یکی از متداول‌ترین نمونه‌های دسترسی مستقیم به برنامه پست الکترونیکی است. کاربر دورکار یک مرورگر وب را اجرا کرده و با استفاده از پروتکل HTTPS به یک سرویس‌دهنده وب که دسترسی به ایمیل‌ها را فراهم می‌کند متصل می‌شود، و سپس سرویس‌دهنده دورکار را احراز اصالت می‌کند. برای مواردی از قبیل پست الکترونیکی دسترسی مستقیم به برنامه یک راه‌کار با انعطاف‌پذیری بالا را ارائه می‌دهد که تقریباً از هر نوع دستگاهی قابل استفاده است. مثال دیگر از دسترسی مستقیم به برنامه، برنامه‌های کاربردی تلفن‌های هوشمند هستند که از طریق HTTPS به یک سرویس ارائه‌شده توسط یکی از سرویس‌دهنده‌های سازمان متصل می‌شوند.

۳- الزامات امنیتی دستگاههای افراد دورکار

دستگاههای کارمندان دورکار در دو دسته کلی رایانه‌های شخصی (دسکتاپ‌ها و لپ‌تاپ‌ها) و دستگاه‌های همراه (رایانه‌های همراه کوچک از قبیل گوشی‌های هوشمند و تبلت‌ها)هستند.

در محیط‌های محاسبات امروز تهدیدات زیادی برای ابزارهای کارمند دورکار وجود دارد. این تهدیدات توسط افراد با انگیزه‌های مختلفی از جمله ایجاد اختلال، سرقت مالکیت معنوی، سرقت هویت و سایر انواع کلاه‌برداری به‌وجود می‌آید. تهدید اصلی در مورد بسیاری از دستگاه‌های کاربران دورکار، بدافزارها شامل از جمله ویروس‌ها، کرم‌ها، تروجان‌ها، روت‌کیت‌ها، جاسوس‌افزارها و ربات‌ها است. بدافزارها می‌توانند دستگاه‌های مشتری را به روش‌های مختلفی از جمله ایمیل، وبگاه‌ها، دانلود فایل و به اشتراک‌گذاری فایل، نرم‌افزارهای نظیر به نظیر و رسانه‌های اجتماعی آلوده کنند. استفاده از رسانه‌های یا دستگاه‌های قابل جابجایی بدون مجوز، مانند فلش مموری‌ها، سازوکار انتقال رایج برای بدافزارها است. یکی دیگر از تهدیدهای رایج در برابر دستگاه‌های کاربر دورکار از بین رفتن یا سرقت دستگاه است. شخصی که دسترسی فیزیکی به یک دستگاه دارد، گزینه‌های زیادی را در اختیار دارد که بتواند برای مشاهده یا کپی کردن اطلاعات ذخیره‌شده روی آن تلاش نماید. مهاجمی که دسترسی فیزیکی دارد همچنین می‌تواند بدافزار را به

دستگاهی اضافه کند که به او امکان دسترسی به داده‌های قابل دسترسی از طریق دستگاه یا داده‌های واردشده به دستگاه را می‌دهد، مانند گذرواژه‌های کاربران که از طریق صفحه کلید لپ‌تاپ تایپ شده‌اند.

اجازه انجام دورکاری و دسترسی از راه دور به منابع محاسباتی یک سازمان یا دسترسی محلی به شبکه‌های سازمان به مهاجمین فرصت بیشتری می‌دهد تا امنیت سازمان را زیر پا بگذارند. هنگامی که یک دستگاه مشتری از دسترسی از راه دور استفاده می‌کند و یا به شبکه محلی دسترسی دارد، در اصل یک توسعه از شبکه خود سازمان است. اگر دستگاه به‌درستی امن‌سازی نشده باشد، نه تنها اطلاعاتی که کاربر دورکار به آن‌ها دسترسی دارد به مخاطره می‌افتد، بلکه سیستم‌ها و شبکه‌های دیگر سازمان نیز در معرض خطر قرار دارند. بنابراین امنیت دستگاه‌های کاربران دورکار باید به‌درستی تأمین شود.

به‌طور کلی، دستگاه‌های کاربران دورکار باید از کنترل‌های امنیتی محلی مشابهی با دستگاه‌های سازمان برخوردار باشند، مانند به‌روزرسانی‌های امنیتی سیستم عامل و برنامه‌های کاربردی، سرویس‌های غیرضروری غیرفعال‌شده و غیره. با این حال، به‌دلیل تهدیداتی که دستگاه‌های مشتری در محیط‌های خارجی با آن روبرو هستند، کنترل‌های امنیتی اضافه‌ای برای آن‌ها توصیه می‌شود، و ممکن است به‌منظور کارکرد مؤثر در محیط‌های دورکاری برخی کنترل‌های امنیتی اضافه تنظیم شوند. به‌عنوان مثال، ذخیره داده‌های حساس در رایانه رومیزی که در دفتر سازمان قرار دارد تفاوت زیادی با ذخیره همان داده‌ها در لپ‌تاپ مورد استفاده در چندین مکان خارجی دارد. در این بخش توصیه‌هایی برای امن‌سازی دستگاه‌های کاربران دورکار و داده‌های موجود در آن‌ها ارائه شده است.

۳-۱- امن‌سازی رایانه‌های شخصی کارمندان دورکار

یکی از مهم‌ترین اقدامات امنیتی برای رایانه شخصی کارمند دورکار، نصب و پیکربندی یک دیواره آتش شخصی مناسب است. در بسیاری از محیط‌ها دیواره‌های آتش شخصی برای متوقف کردن تهدیدات امنیتی مبتنی بر شبکه مورد نیاز است. اگر یک دیواره آتش شخصی برای همه محیط ها یک سیاست واحد دارد، به احتمال زیاد در بعضی مواقع بسیار محدودکننده است، مانند زمانی‌که کارمند در شبکه داخلی سازمان وجود دارد، و در سایر مواقع به اندازه کافی محدود نیست، مانند زمانی‌که کارمند در یک شبکه بی‌سیم خارجی شخص ثالث قرار دارد. بنابراین باید از دیواره‌های

آتش شخصی که قادر به پشتیبانی از سیاست‌های متعدد هستند استفاده شود و در محیط سازمان و محیط خارجی به‌درستی پیکربندی شود.

مورد مهم دیگر در رایانه‌های شخصی دورکاری استفاده از به‌روزرسانی‌های امنیتی سیستم عامل و برنامه‌های کاربردی است. برای رایانه‌های شخصی دورکاری که توسط کاربران آن‌ها امن‌سازی شده‌اند بهتر است پیکربندی سیستم عامل و برنامه‌های کاربردی به‌صورتی انجام شود که به‌طور خودکار با سرویس‌های آنلاین فروشندگان تماس بگیرند تا به‌روزرسانی‌ها را بررسی کرده و آن‌ها را دانلود و نصب نمایند. سیاست سازمان برای دریافت به‌روزرسانی‌ها ممکن است متفاوت باشد. به‌عنوان مثال، ممکن است سازمان بخواهد برای همه رایانه‌های شخصی خود از یک سیستم متمرکز مدیریت به‌روزرسانی استفاده کند، اما اگر رایانه‌های دورکاری به چنین سیستمی متکی باشند ممکن است به‌روزرسانی‌ها را فوراً دریافت نکنند و بنابراین رایانه شخصی در معرض تهدیداتی قرار می‌گیرد. سازمان‌ها همچنین باید کاربران خود را تشویق کنند که قبل از مسافرت یا رفتن به سایر محیط‌های کنترل نشده، رایانه‌های شخصی دورکاری خود را به‌طور کامل به‌روزرسانی کنند.

سایر اقدامات امنیتی که برای دورکاری مهم هستند شامل موارد زیر است:

- برای هر شخصی که از رایانه شخصی دورکاری استفاده می‌کند یک حساب کاربری جداگانه با امتیازات محدود وجود داشته باشد. دورکارها باید برای کار معمولی خود از حساب‌های دارای امتیازات محدود خود استفاده کنند و فقط برای کارهایی که نیاز به دسترسی در سطح مدیر دارند، مانند برخی به‌روزرسانی‌های نرم‌افزاری، از یک حساب مدیریتی جداگانه استفاده کنند. این امر احتمال این‌که مهاجمان بتوانند ورود با سطح دسترسی مدیر به یک رایانه شخصی را به‌دست بیاورند، را کاهش می‌دهد.
- قفل نشست‌ها را اعمال کنید، که از دسترسی به رایانه شخصی پس از گذشت مدت زمانی از بی‌کار ماندن (مانند ۱۵ دقیقه) جلوگیری می‌کند و یا به کاربر اجازه می‌دهد که در صورت تقاضا نشست را قفل کند. بعد از این‌که یک نشست قفل شد، دسترسی به رایانه شخصی فقط از طریق انجام احراز اصالت قابل بازیابی است. قفل نشست اغلب بخشی از نرم‌افزار محافظ صفحه نمایش[۸] است. این امر مانع از این می‌شود که یک مهاجم در مجاورت فیزیکی یک رایانه به‌آسانی به نشست فعلی دسترسی پیدا کند. با این حال، مهاجمی که رایانه

[۸] Screen Saver Software

شخصی را سرقت می‌کند یا برای مدت زمان طولانی به آن دسترسی دارد خنثی نمی‌شود. قفل نشست را می‌توان به روش‌های مختلف دور زد.

- با استفاده از قفل کابل یا سایر عوامل بازدارنده در سرقت، رایانه‌های شخصی دورکاری را از لحاظ فیزیکی امن‌سازی کنید. این مورد برای رایانه‌های دورکاری در محیط‌های خارجی غیرقابل اعتماد از اهمیت زیادی برخوردار است. همچنین، در این محیط‌ها اگر قرار است رایانه بدون مراقبت باقی بماند آن را خاموش کنید.

۳-۲- امن‌سازی دستگاه‌های همراه دورکاری

کارمندان دورکار می‌توانند امنیت دستگاه‌های همراه خود را از طریق نرم‌افزار مدیریت دستگاه همراه سازمانی، به‌صورت مرکزی مدیریت کنند. سازمان‌ها باید از هرگونه امکانات مدیریت امنیتی موجود، به‌ویژه برای دستگاه‌های تحت کنترل سازمان، استفاده کنند. به‌عنوان مثال، با محدودکردن نصب و استفاده از برنامه‌های شخص ثالث، یا با تهیه یک فروشگاه برنامه با برنامه‌های مجاز، به‌صورتی‌که اجازه دانلود و نصب برنامه فقط از این فروشگاه به کاربر داده شود. با این وجود، بسیاری از دستگاه‌ها باید به‌صورت دستی امن‌سازی شوند. قابلیت‌های امنیتی و اقدامات مناسب با توجه به نوع دستگاه و محصولات خاص متفاوت است. بنابراین سازمان‌ها باید مدیران دستگاه‌ها و کاربرانی که وظیفه امن‌سازی دستگاه‌های همراه دورکاری دارند را در مورد چگونگی انجام امن‌سازی راهنمایی کنند.

- قابلیت‌های شبکه دستگاه‌های همراه را محدود کنید. این امر به‌ویژه برای دستگاه‌هایی که چندین قابلیت بی‌سیم دارند اهمیت دارد. شخص دورکار ممکن است حتی نداند که برخی از پروتکل‌های بی‌سیم، مانند بلوتوث و شبکه بی‌سیم مشترک، دستگاه را در معرض دسترسی مهاجمان قرار می‌دهند.
- برای دستگاه‌هایی که با تهدیدهای بدافزار مواجه هستند، برنامه‌های ضد بدافزار را اجرا کنید. دستگاه‌هایی که به اینترنت متصل می‌شوند دارای دیواره‌های آتش شخصی هستند. این دیواره‌های آتش باید برای جلوگیری از حملات و دسترسی غیرمجاز فعال شوند.
- تعیین کنید که آیا سازنده دستگاه به‌روزرسانی‌ها و وصله‌های امنیتی را ارائه می‌دهد. در این صورت، اطمینان حاصل کنید که به‌روزرسانی‌ها و وصله‌های امنیتی، برای محافظت از دستگاه در برابر حملات در برابر آسیب‌پذیری‌های شناخته‌شده، بلافاصله اعمال می‌شوند.

- داده‌های ذخیره‌شده در رسانه‌های ذخیره‌سازی داخلی و قابل جابجایی را به‌شدت رمزنگاری کنید.
- قبل از دسترسی به منابع سازمان، به گذرواژه/کد عبور و/یا احراز اصالت به روش‌های دیگر نیاز وجود داشته باشد.
- با استفاده از لیست سفید یا لیست سیاه، برنامه‌های کاربردی که اجازه نصب بر روی دستگاه دارند را محدود کنید.

سازمان‌ها باید مزایای استفاده از راه‌حل‌های مدیریت دستگاه‌های همراه (MDM[۹])، راه‌حل‌های مدیریت برنامه‌های کاربردی همراه (MAM[۱۰]) و سایر فناوری‌ها برای کنترل استفاده از دستگاه‌های همراه را در نظر بگیرند. راه‌حل‌های MDM قادر به اعمال انواع سیاست‌های امنیتی به نمایندگی از سازمان هستند. به‌عنوان مثال، از نرم‌افزار MDM غالباً برای الزام استفاده از پین برای باز کردن قفل دستگاه همراه، فعال‌کردن فناوری‌های رمزنگاری برای محافظت از داده‌های حساس ذخیره‌شده در دستگاه همراه و برای تعیین این‌که آیا دستگاه همراه روت شده است، استفاده می‌شود. نرم‌افزار MDM همچنین می‌تواند پاک کردن از راه دور را انجام دهد. این امر برای جلوگیری از دسترسی غیرمجاز به داده‌های حساس موجود در دستگاه، در صورت گم‌شدن یا دزدیده‌شدن، می‌تواند مفید باشد. سازمان می‌تواند خط‌مشی‌های مختلف MDM را برای دسته‌های مختلف از دستگاه‌های همراه، از جمله دستگاه‌های همراه سازمان، دستگاه‌های همراه کنترل‌شده توسط شخص ثالث و BYOD تنظیم کند تا سطح دسترسی متفاوت هر نوع دستگاه را در نظر بگیرد. نرم‌افزار MAM محیطی را فراهم می‌کند که برنامه‌ها و داده‌های سازمانی را از بقیه دستگاه جدا می‌کند. برای دسترسی به محیط سازمانی، که برای محافظت از داده‌ها و برنامه‌های حساس سازمان رمزنگاری نیز می‌شود، و به حداقل رساندن نشت داده‌ها از آن برنامه‌ها به سایر برنامه‌ها و سرویس‌های در حال اجرا در دستگاه، بهتر است احراز اصالت قوی وجود داشته باشد. در صورت گم‌شدن دستگاه یا ترک سازمان توسط کارمند، می‌توان محیط حفاظت‌شده را از راه دور پاک کرد و داده‌های سازمان را از بین برد.

۳-۳- حفاظت از داده‌های دستگاه‌های کارمندان دورکاری

دورکاری اغلب شامل ایجاد و ویرایش اطلاعات مربوط به کار مانند ایمیل، اسناد word و صفحه گسترده است. از آن‌جایی‌که این داده‌ها دارای اهمیت هستند، باید با آن‌ها مانند سایر دارایی‌های مهم سازمان رفتار شود. دو موردی که یک سازمان می‌تواند برای محافظت از داده‌های مربوط به دستگاه‌های دورکاری انجام دهد این است که آن را در

[۹] Mobile Device Management
[۱۰] Mobile Application Management

دستگاه دورکاری محافظت کند و به‌صورت دوره‌ای از آن در مکانی که توسط سازمان کنترل می‌شود پشتیبان تهیه نماید. سازمان‌ها همچنین می‌توانند اجازه ندهند که اطلاعات سازمان در دستگاه‌های دورکاری ذخیره شود، و آن را به‌طور متمرکز در سازمان ذخیره کنند.

اطلاعات حساس، مانند انواع خاصی از اطلاعات شخصی قابل شناسایی (PII) (به‌عنوان مثال سوابق پرسنلی، سوابق پزشکی، سوابق مالی)، که در دستگاه‌های دورکاری ذخیره شده یا به/از آن فرستاده می‌شوند باید محافظت شوند تا طرفین مخرب نتوانند به آن‌ها دسترسی پیدا کرده یا آن‌ها را تغییر دهند. به‌عنوان مثال، کارمندان دورکار غالباً فراموش می‌کنند که ذخیره‌سازی اطلاعات حساس بر روی سی دی که با دستگاه آن‌ها حمل می‌شود، یا چاپ اطلاعات بر روی چاپگر عمومی، هم می‌تواند اطلاعات را به روش‌هایی که در محیط معمولی شرکت مهم نیستند، افشا نماید. انتشار غیرمجاز اطلاعات حساس می‌تواند به اعتماد عمومی به یک سازمان آسیب برساند، رسالت سازمان را به خطر بیندازد، یا در صورت انتشار اطلاعات شخصی به افراد آسیب برساند.

۳-۳-۱- رمزنگاری داده‌ها در حالت استراحت

تمام دستگاه‌های دورکاری، صرف‌نظر از اندازه و یا موقعیت مکانی آن‌ها، می‌توانند سرقت شوند. ممکن است برخی از سارقان بخواهند محتوای داده‌های دستگاه را بخوانند و احتمالاً از این داده‌ها برای مقاصد جنایی استفاده کنند. برای جلوگیری از این امر، سازمان باید سیاستی را برای رمزنگاری کلیه داده‌های حساس دستگاه و رسانه‌های قابل جابجایی استفاده‌شده توسط دستگاه، در هنگام استراحت آن، داشته باشد. ایجاد و استفاده از کلیدهای رمزنگاری برای رمزنگاری داده‌های دورکاری در حالت استراحت باید همان سیاست‌هایی را دنبال کند که سازمان برای سایر کلیدهای خود که محافظت از داده‌ها را در حالت استراحت انجام می‌دهند دارد.

روش‌های زیادی برای محافظت از داده‌ها در حالت استراحت وجود دارد و بیشتر آن‌ها به نوع دستگاه یا رسانه قابل جابجایی که محافظت می‌شود بستگی دارد. اکثر سیستم‌های عامل دارای یک سازوکار خاص خود برای رمزنگاری داده‌ها هستند، همچنین تعداد زیادی برنامه شخص ثالث نیز وجود دارند که قابلیت‌های مشابهی را ارائه می‌دهند.

۳-۳-۲- استفاده از ماشین‌های مجازی

اگر یک سازمان کنترل مستقیم بر یک دستگاه دورکاری داشته باشد، می‌تواند خط‌مشی‌های خود برای دسترسی از راه دور، به‌روزرسانی و غیره را اعمال کند. در مورد سایر دستگاه‌های دورکاری، مانند رایانه‌های شخصی BYOD، سازمان توانایی محدودی در اجرای سیاست‌های امنیتی دارد. یک روش برای کنترل محیطی که یک کارمند دورکار در آن فعالیت می‌کند اجرای یک ماشین مجازی (VM[۱۱]) بر روی رایانه شخصی دورکار است. این کار معمولاً با اجرای یک برنامه ابرناظر[۱۲] ماشین مجازی در سیستم عامل رایانه شخصی کارمند دورکار انجام می‌شود، اما برخی از رایانه‌های شخصی دورکاری جدیدتر امکان نصب ابرناظر به‌جای سیستم عامل رایانه شخصی را دارند.

کاربر یک تصویر ماشین مجازی را در محیط ماشین مجازی اجرا می‌کند. این تصویر درست مانند یک کامپیوتر کامل با سیستم عامل و برنامه‌های کاربردی عمل می‌کند. برای استفاده از تصاویر ماشین مجازی برای اجرای سیاست‌های دورکاری، سازمان یک تصویر ماشین مجازی را توزیع می‌کند که به‌گونه‌ای پیکربندی شده است که با تمام سیاست‌های امنیتی مورد نظر سازگار باشد. کارمند دورکار تصویر ماشین مجازی را در رایانه دورکاری اجرا می‌کند. در صورت نیاز به به‌روزرسانی تصویر ماشین مجازی، سازمان تصویر جدیدی را به کارمندان دورکاری خود توزیع می‌کند. استفاده از ماشین مجازی برای پشتیبانی از امنیت دورکاری تا زمانی کار می‌کند که خود رایانه دورکاری هیچ بدافزاری نداشته باشد که به ماشین مجازی حمله کند. برای ابرناظرهایی که در سیستم عامل میزبان کار می‌کنند، هرگونه تهدید در سیستم عامل میزبان می‌تواند بر امنیت ماشین مجازی و تصویر ماشین مجازی تأثیر بگذارد.

دیسک‌های ماشین مجازی دقیقاً مانند دیسک‌های یک کامپیوتر معمولی عمل می‌کنند، بنابراین سازمان‌ها باید برای داده‌های دورکاری که در یک تصویر ماشین مجازی ذخیره می‌شوند هم خط‌مشی‌هایی داشته باشند. تصاویر ماشین مجازی می‌توانند به‌هنگام عدم استفاده در رایانه دورکاری رمزنگاری شوند، و رمزگشایی آن‌ها قبل از بوت‌کردن تصویر تنها در صورتی انجام شود که کاربر اطلاعات احراز اصالت صحیح را ارائه دهد. اگر تصویر ماشین مجازی رمزنگاری شود، شخص غیرمجازی که به دستگاه دورکاری دسترسی پیدا می‌کند، قادر به خواندن داده‌های ذخیره شده در تصویر ماشین مجازی نخواهد بود. یک تصویر ماشین مجازی می‌تواند چندین دیسک داشته باشد و برخی از آن‌ها (که شامل داده‌های کاربر هستند) رمزنگاری شوند. اگر کارمند دورکار داده‌های خود را روی دیسک رمزنگاری شده در

[۱۱] Virtual Machine
[۱۲] Hypervisor

داخل ماشین مجازی ذخیره کند، دقیقاً مشابه با حالتی خواهد بود که داده‌ها بر روی یک دیسک رمزنگاری‌شده مستقیم بر روی رایانه دورکار ذخیره شوند.

سازمان‌ها باید تمام تصاویر ماشین مجازی را که برای دورکاری استفاده می‌شود را رمزنگاری کنند تا خطر افشا را کاهش دهند. این امر می‌تواند با استفاده از رمزنگاری کامل دیسک، رمزنگاری فایل یا سایر موارد محقق شود. برای موقعیت‌های پرخطر که شامل دسترسی به اطلاعات بسیار حساس است، سازمان ها باید هر تصویر ماشین مجازی را که برای دورکاری استفاده می‌کنند رمزنگاری کنند؛ همچنین ممکن است در چنین مواردی یک لایه دوم محافظت از طریق رمزنگاری کامل دیسک نیز ارائه شود.

۳-۳-۳- پشتیبان‌گیری از داده‌های روی دستگاه‌های دورکاری

بیشتر سازمان‌ها سیاست‌هایی برای تهیه نسخه پشتیبان از داده‌ها به‌طور منظم دارند. چنین سیاست‌های پشتیبان‌گیری باید داده‌های روی رایانه‌های دورکاری و دستگاه‌های همراه را نیز پوشش دهند. با این حال، چنین سیاستی ممکن است به مقررات مختلفی برای پشتیبان‌گیری‌هایی که در خارج از سازمان انجام می‌شود، نسبت به پشتیبان‌گیری‌هایی که در درون سازمان انجام می‌شود، نیاز داشته باشد. اگر داده‌هایی که باید از آن‌ها پشتیبان گرفته شود حاوی اطلاعات حساس باشند یا به دلایل دیگر محرمانه باشند، در صورت انجام پشتیبان‌گیری در یک مکان خارجی، ملاحظات امنیتی دیگری وجود دارد.

اگر از داده‌ها از راه دور، از دستگاه دورکاری به یک سیستم در سازمان، پشتیبان گرفته می‌شود، باید ارتباطات حامل آن داده ها رمزنگاری شده و صحت آن‌ها تأیید شود. اگر از داده‌ها به‌صورت محلی پشتیبان تهیه شود، به‌عنوان مثال در رسانه‌های قابل جابجایی مانند سی دی یا فلش درایو، باید از نسخه پشتیبان حداقل به اندازه‌ی نسخه‌ی اصلی محافظت شود. به‌عنوان مثال، اگر داده‌های اصلی رمزنگاری شده‌اند، باید داده‌های موجود در نسخه پشتیبان نیز رمزنگاری شوند. اگر داده‌های اصلی به شکل قابل حمل رمزنگاری شوند، مانند رمزنگاری دیسک مجازی یا تصویر ماشین مجازی رمزنگاری‌شده، ممکن است کپی کردن آن داده‌ی رمزنگاری‌شده بر روی رسانه پشتیبان کافی باشد. با این حال، برای شکل‌های غیرقابل حمل از رمزنگاری ذخیره‌سازی، مانند رمزنگاری کامل دیسک، لازم است داده‌ها روی دستگاه دورکاری رمزگشایی شوند و سپس برای ذخیره‌سازی بر روی رسانه پشتیبان رمزنگاری شوند.

۴- توصیه‌های عمومی برای کارمندان دورکاری

در این قسمت به مروری بر توصیه‌های عمومی که سازمان‌های باید به کارمندان خود به‌منظور انجام دورکاری داشته باشند می‌پردازیم. بدیهی است که هر چه این توصیه‌ها، و سایر مواردی که به‌صورت مفصل در قسمت‌های قبل توضیح داده شد، با جدیت بیشتری از سوی سازمان به کارمندان آموزش داده شود، امکان وقوع مخاطرات امنیتی از قبیل افشای اطلاعات سازمان یا کارمندان کمتر می‌شود. لازم به ذکر است مباحث قسمت‌های قبل این توصیه‌ها و سایر موارد مربوط به امن‌سازی ارتباطات راه دور را پوشش می‌دهند ولی به‌دلیل اهمیت موضوع در این قسمت به‌صورت خلاصه و فهرست‌وار مهم‌ترین توصیه‌های عمومی که بایستی به کارمندان توسط سازمان آموزش داده شوند، ارائه می‌شود.

- دورکاری در یک فضای اختصاصی و مجزا انجام شود که امنیت کافی برای نگه‌داری مستندات سازمان را داشته باشد.
- از پاسخ‌دادن به تماس‌های تصویری غیرمنتظره در هنگام دورکاری اجتناب شود.
- کنفرانس ویدئویی تنها با افراد مطمئن و مورد تأیید شرکت انجام شود.
- امنیت فیزیکی لازم برای دستگاه دورکاری (و سایر مستندات مرتبط با دورکاری) وجود داشته باشد، به‌گونه‌ای که احتمال گم‌شدن یا سرقت آن‌ها به حداقل برسد. همچنین، دستگاه و مستندات دورکاری بایستی از دسترس بچه‌ها دور نگه داشته شوند.
- به‌هنگام ترک دستگاه حتماً آن را قفل کرده و در صورت امکان محیط کار خود را نیز قفل نماید.
- در صورت امکان، از فیلترهای صفحه نمایش، به منظور سخت‌تر کردن حملات shoulder surfing استفاده شود و یا این‌که دقت شود که در محیط‌های عمومی کسی به صفحه نمایش دستگاه اشراف نداشته باشد. (به‌هیچ عنوان تصویری از صفحه نمایش دستگاه در حال کارکردن در فضای مجازی منتشر نشود.)
- دستگاه دورکاری با اعضای خانواده یا دوستان به اشتراک گذاشته نشود.
- از دستگاه دورکاری (به‌ویژه اگر متعلق به سازمان باشد) تنها برای فعالیت‌های مرتبط با کار استفاده شود و استفاده شخصی از صورت نگیرد.
- از ایمیل‌های شخصی برای اهداف کاری استفاده نشود.
- به‌منظور جلوگیری از حملات فیشینگ بر روی هیچ‌گونه لینک مشکوکی، به‌هیچ عنوان، کلیک نشود.

- ضمیمه‌های ایمیل‌ها قبل از دانلود حتما اسکن شوند (به‌منظور شناسایی ویروس‌ها یا بدافزارها).
- حتماً از روش‌های مورد تأیید سازمان (به‌عنوان مثال، VPN اختصاصی) برای ارتباطات دورکاری استفاده شود.
- در صورت استفاده از شبکه Wi-Fi خانگی حتما امن‌سازی آن به‌صورت سختگیرانه انجام شود (استفاده از SSID واحد و مخفی کردن آن، استفاده از گذرواژه با پیچیدگی زیاد، استفاده از WPA۲ یا WPA۳).
- از گذرواژه‌های پیچیده استفاده شود (طول بیشتر از ۸ کاراکتر که شامل عدد، حروف بزرگ و کوچک و کاراکترهای خاص باشد).
- گذرواژه با دیگران (حتی اعضای خانواده) به اشتراک گذاشته نشود.
- از نوشتن و یادداشت گذرواژه اجتناب شود.
- از انتخاب گذرواژه‌های یکسان برای حساب‌های کاربری و مقاصد مختلف اجتناب شود.
- از احراز اصالت دو یا چند عامله استفاده شود.
- فایل‌ها قبل از به اشتراک‌گذاری آن‌ها اسکن شوند و همچنین فایل‌های از منابع ناشناخته به‌هیچ عنوان به اشتراک گذاشته نشوند.
- تنها از برنامه‌های کاربردی ابری مورد تأیید برای ذخیره و به اشتراک‌گذاری اطلاعات کاری استفاده شود.
- قبل از انجام هرگونه نصب یا دانلود از سازمان اجازه گرفته شود.
- آگاهی لازم در مورد حملات و کلاه‌برداری‌های سایبری وجود داشته باشد. روش‌های بسیار متنوعی برای کلاه‌برداری‌های سایبری وجود دارد. به‌عنوان مثال، از طریق شبکه‌های اجتماعی، ایمیل یا پیامک ممکن است در ازای دریافت یک خدمت اطلاعاتی از قربانی گرفته شود، یا ایمیل‌ها یا لینک‌های فیشینگ که معمولاً بسیار فریبنده هستند (به‌عنوان مثال، در شرایط فعلی در سراسر دنیا انجام حملات فیشینگ از طریق لینک‌های به ظاهر مرتبط با بیماری کورونا به‌شدت افزایش یافته است) و غیره.
- از کانال‌های مورد تأیید سازمان برای انتقال اطلاعات استفاده شود.
- به‌روزرسانی‌های سیستم عامل، برنامه‌های کاربردی، نرم‌افزارها و آنتی‌ویروس‌ها به‌صورت منظم انجام شود.
- در یک مکان امن از داده‌ها به‌صورت مرتب پشتیبان گرفته شود.
- از دیواره آتش، به‌صورت مناسب، استفاده شود.

- هرگونه فعالیت یا اتفاق مشکوک سریعاً به مدیر سیستم یا بخش امنیت اطلاعات سازمان اطلاع داده شود.

۵- نتیجه‌گیری

دسترسی به منابع سازمان از راه دور امکان دورکاری را فراهم می‌کند اما خطرات امنیتی را نیز افزایش می‌دهد. سازمان‌ها باید با دقت بین مزایای دسترسی از راه دور به منابع و تأثیر احتمالی این دسترسی در به مخاطره افتادن این منابع تعادل برقرار کنند. برای کاهش خطر، سازمان‌ها باید اطمینان حاصل کنند که منابع داخلی که برای دسترسی از راه دور از طریق دورکاری در دسترس قرار گرفته‌اند در برابر تهدیدات خارجی مقاوم‌سازی شده و دسترسی به منابع به حداقل مورد نیاز محدود شده است. همچنین، سازمان‌ها باید اطمینان حاصل کنند که توصیه‌های امنیتی لازم را به کارمندان دورکار خود داشته و دستگاه‌های مورد استفاده توسط کارمندان دورکار نیز به‌اندازه‌ی کافی امن‌سازی شده است.

۶- مراجع

[۱] Scarfone, Karen, Jeffrey Greene, and Murugiah Souppaya. "Security for enterprise telework, remote access, and bring your own device (BYOD) solutions". No. ITL Bulletin March ۲۰۲۰. National Institute of Standards and Technology, ۲۰۲۰.

[۲] Souppaya, Murugiah, and Karen Scarfone. "Guide to enterprise telework, remote access, and bring your own device (BYOD) security". No. NIST Special Publication (SP) ۸۰۰-۴۶ Rev. ۲. National Institute of Standards and Technology, ۲۰۱۶.