تاریخ دریافت: ۹٤/۵/۱۵
تاریخ تأیید: ۹٤/۹/۲۰

حفاظت از کارکنان در فضای مجازی

رضا قیاسی[۱]
امین ملکی[۲]

چکیده

با توجه به اهمیت دنیای مجازی در عصر حاضر و رشد سریع و در عین حال ناموازن ساختار فضای تبادل اطلاعات، این بستر به یکی از نقاط بالقوه آسیب‌پذیر و خطرناک در جهان مبدل شده است. ضرورت توجه و پرداخت سریع و نظام‌مند، معقول و هدفمند؛ مصون‌سازی این بستر از تهدیدهای موجود به‌منظور حفظ کارکنان در مقابل آسیب‌های این فضا و حریم کارکنان را می‌طلبد. عنوان دروازه‌ی جهنم، بیان کننده‌ی مخاطرات این پدیده‌ی نوظهور است و می‌تواند نگرانی‌های اخلاقی و امنیتی فراوانی را در سازمان تداعی کند. دشمنان متخاصم از این راه، آسیب‌های جدی را در ابعاد مختلف بر پیکره‌ی سازمان اطلاعاتی پلیس وارد می‌سازند؛ در بعد امنیتی و اطلاعاتی، به دنبال کسب اطلاعات و انتشار آن اخبار در زیر نقاب جاسوسی اینترنتی با آموزش‌های مخرب خرابکاری، به‌دنبال تضعیف و نقصان سامانه‌های امنیتی سازمان هستند؛ در بعد اجتماعی با فراهم آوردن زمینه‌های غیراخلاقی بین جوانان، به ایجاد ارتباطات نامتعارف بین آنها پرداخته و به مسخ هویت و شخصیت آنان اقدام می‌کنند؛ این زمینه‌های غیراخلاقی، بنیان‌های خانوادگی را مورد تهدید قرار داده و با شکل‌گیری خرده فرهنگ‌های مختلف، شکاف بین نسل‌ها را افزایش می‌دهد.

امروزه حضور پلیس در قلمروی مجازی برای واپایش بسیاری از ناهنجاری‌هایی که ممکن است در این محیط شکل بگیرد، امری ضروری است. در این تحقیق برآنیم که با روش توصیفی– تحلیلی به سؤال‌های زیر پاسخ دهیم "مهم‌ترین راه‌کارهای علمی و عملی مناسب برای افزایش هشیاری و حفاظت از کارکنان در فضای سایبر کدام است؟ راه‌کارهای کاربردی مناسب برای شناسایی تهدیدهای بالقوه کارکنان در فضای تبادل اطلاعات کدام است؟

کلید واژه

آسیب‌ها، تهدیدها، حفاظت کارکنان، فضای تبادل اطلاعات،

---

۱. کارشناس ارشد اطلاعات پلیس فتا ناجا.
۲. کارشناس ارشد مهندسی نرم‌افزار .

مقدمه

بررسی و شناخت علل و عوامل آسیب‌پذیری کارکنان در فضای مجازی یکی از مهم‌ترین موضوع‌های فناوری است. پیش‌بینی تمهیدهای لازم در جلوگیری از آسیب‌پذیری کارکنان یکی از نیازهای بسیار مهم در فرایند پیشگیری از این رخدادهاست. در بسیاری از موارد، کاربران اینترنت در رایانه‌ی شخصی خود، اطلاعات با ارزشی مانند: فیلم و تصاویر و اطلاعات سازمانی و طبقه‌بندی شده و... را نگهداری می‌کنند (آیکاو، ۱۳۸۳). با به اشتراک‌گذاری، انتقال و ذخیره‌ی فزاینده‌ی اطلاعات حساس در سامانه‌های متصل به اینترنت، موارد سوءاستفاده‌های فضای مجازی به شکلی چشمگیر، افزایش یافته‌اند. استفاده از ارتباطات شبکه محور و شبکه‌های اجتماعی، فرصت‌های بی‌سابقه‌ای را برای جاسوسی دستگاه‌های اطلاعاتی در کشورها به‌وجود آورده است. در یک گزارش به‌طور مشخص، توانایی رشد یافته‌ی چین در بهره‌برداری از شبکه‌های رایانه‌ای را، پشتیبان مستقیم عملیات اطلاعاتی علیه دولت و صنایع دفاعی امریکا می‌داند و آن را یک " کارزار دراز مدت و دشوار بهره‌برداری از شبکه‌های رایانه‌ای" که بسیار هدایت شده است، توصیف می‌کند (احمدوند، ۱۳۸۹).

محیط فضای مجازی با ارائه‌ی سرویس‌های بی‌دلیل و متنوع، بستر مناسبی را برای مبادله‌ی اطلاعات و توسعه‌ی دانش و دانایی فراهم کرده و بسیاری از محققان و دانشمندان، با بهره‌گیری از امکانات متنوع این بستر ارتباطی، دامنه‌ی پژوهش و تحقیقات خود را در سراسر جهان گسترش داده و به مبادله‌ی اطلاعات و دانش می‌پردازند اما محیط اشاره شده، به موازات مزایا و فرصت‌هایی که برای توسعه‌ی دانش و دانایی فراهم کرده، تهدیدهایی را نیز متوجه‌ی کاربران و اطلاعات آنها ساخته است (آشوری، ۱۳۸٦).

اهمیت مهندسی ایمن‌سازی محیط فضای مجازی در حدی است که پنتاگون در سند امنیت ملی بر لزوم پیش‌بینی تدابیر بازدارنده و پیش‌دستانه‌ی مناسب برای مقابله با تهدیدهای فضای مجازی کشور چین که در حوزه‌ی شبکه‌های جاسوسی مجازی، پیشرفت چشمگیری داشته تأکید کرده است. از مهم‌ترین مصادیق آن می‌توان به نفوذ

و دست‌یابی جاسوسان شبکه‌ای پکن به اطلاعات محرمانه‌ی ناسا اشاره کرد (افتخاری، ۱۳۹۰).

مداخله فضای مجازی به چند دلیل، کم‌کم به روش ترجیحی انجام جاسوسی بدل می‌شود. مزیت اصلی این روش آن است که عملیات در فضای مجازی، امکان بیشتری برای ناشناس ماندن به دشمن می‌دهد؛ چرا که بسیاری از مداخله‌ها کشف نمی‌شوند یا ردیابی آنها دشوار است و به این ترتیب، مخاطره‌ی افشای عملیات که ملازم همیشگی استخراج پنهانی اطلاعات و توسعه‌ی منابع انسانی است، کاهش می‌یابد. همچنین با توجه به مقادیر عظیم داده‌هایی که در سامانه‌های شبکه‌ای ذخیره می‌شوند، دستاورد اطلاعاتی یک مداخله‌ی موفق، به‌طور بالقوه می‌تواند بیشتر از اطلاعات کسب شده به واسطه‌ی سال‌ها فعالیت حساب شده منابع انسانی باشد. گمان می‌رود که چین تنها در یکی از این نوع حمله‌ها، چند ترابایت داده از شبکه‌های دولتی امریکا را به‌دست آورده باشد. مداخله‌ی فضای مجازی، راهبردی به‌طور نسبی کم مخاطره و پرمنفعت برای جمع‌آوری کنندگانی است که دانش فنی ترتیب دادن چنین کارزاری را دارند. ما در این تحقیق می‌خواهیم چگونگی استفاده از راه‌کارهای علمی و عملی و منطقی مناسب برای افزایش هشیاری ضداطلاعاتی و حفاظت اطلاعاتی را برای کارکنان توضیح دهیم.

کلیات

هدف‌های تحقیق

هدف اصلی

- رسیدن به راه‌کارهای علمی و عملی مناسب برای افزایش هشیاری و حفاظت از اطلاعات کارکنان در فضای مجازی.

هدف‌های فرعی

- نقش ضداطلاعات در جلوگیری از آسیب‌پذیری و تهدیدهای بالقوه در فضای مجازی برای کارکنان
- نقش حفاظت اطلاعات در جلوگیری از زیرپاکشی در فضای مجازی

- شناسایی تهدیدهای بالقوه برای کارکنان در فضای مجازی
- شناسایی راه‌کارهای کاربردی برای حفظ امنیت اطلاعات در برابر تهدیدهای فضای مجازی

روش و نوع تحقیق

از آنجا که تاکنون در خصوص این موضوع، تحقیقی صورت نگرفته است؛ در نظر است تا از دستاوردهای تحقیق برای کاربردی شدن نقش ضداطلاعات و حفاظت اطلاعات در جلوگیری از آسیب‌پذیری کارکنان استفاده شود. بنابراین نوع تحقیق کاربردی و روش تحقیق توصیفی– تحلیلی است.

سابقه و پیشینه تحقیق

«استیو مانسر» و «سارا نتلتون» (۲۰۰۱) معتقدند جنبه‌ی غیربیرونی بودن فضای مجازی و غیرقابل تطبیق بودن واقعیت مجازی با واقعیت واقعی، امری نوین و خطرناک است و برای تبیین شرایط جدید حاکم بر رسانه‌ها از اصطلاح دوجهانی شدن استفاده کرده‌اند. جهان مجازی در کنار جهان واقعی وجود دارد و به جزئی از آن تبدیل شده است.

«کشتی ارای» و «اکبریان» (۱۳۹۰) با معرفی عصر جدید به‌عنوان عصر پرشتاب ارتباطات، ورود بسیار ساده و سریع، حداقل محدودیت برای دسترسی، برقراری ارتباط با سراسر دنیا به اشکال مختلف و نبود محدودیت زمانی و مکانی، دسترسی به پایگاه‌های اطلاعاتی مختلف و شرکت در فعالیت‌های اقتصادی، علمی، فرهنگی، هنری، مذهبی و ... را از ویژگی‌های بی‌بدیل این فضا برشمرده‌اند.

«یاسمی نژاد»، «آزادی» و «امویی» (۱۳۹۰) در پژوهش خود به این نتیجه دست یافتند که فضای مجازی می‌تواند امنیت اجتماعی را مورد تهدید قرار دهد؛ زیرا اینترنت با وجود این که می‌تواند به‌عنوان ابزاری قدرتمند در عرصه‌ی اطلاع‌رسانی به‌کار گرفته شود تا آن‌جا که گاهی از آن به‌عنوان انفجار اطلاعات هم نام برده می‌شود ولی این فناوری مدرن با تمام فوایدی که دارد، تهدیدها و خطرهایی نیز برای جامعه و بشر داشته است؛ به‌طوری که امروزه، بخش عمده‌ای از جرایم مربوط

به حوزه‌ی رایانه، اینترنت و فضای مجازی که امنیت اجتماعی را هدف قرار داده، است.

«لیندلاف» (۲۰۰۲) ارتباطات رایانه‌ای را بسیار متفاوت از سایر ارتباطات می‌داند و معتقد است این‌گونه ارتباطات باید با یک روش‌شناسی متفاوت از بقیه‌ی روش‌ها، مورد تجزیه و تحلیل قرار گیرند. «لیندلاف» در این مورد معتقد به یک رویکرد ساختار اجتماعی است؛ رویکرد ساختار اجتماعی، عوامل غیرانسانی را هم در ارتباطات دخیل می‌داند.

«ابری» (۱۳۸۷) نقش مثبت فضای مجازی را در عرصه‌ی ظهور خلاقیت، مورد تأکید قرار داده است؛ زیرا فناوری دیجیتالی و جامعه‌ی شبکه‌ای، افراد را به‌سوی زندگی‌ای سوق داده است که در آن می‌توانند با ایفای نقشی فعال و خلاق، به‌صورت فردی یا جمعی در ساختن چیزی جدید سهیم باشند، در فرایند هم‌آفرینی شرکت کنند و به خودیابی خویشتن کمک کنند. کیفیت آزادی‌بخشی اینترنت، کاربران اینترنتی را دعوت می‌کند تا به تفکر، تجربه، بازی، فعالیت‌های گروهی و ارتباط بپردازند. اینترنت همواره محیطی را خلق کرده است که همگان می‌توانند با تکیه بر توانایی‌ها و استعدادهای خود، دست به ابداع و خلاقیت بزنند. از میان رفتن محدودیت مکان، زمان، نبود واپایش و انتقاد، ناشناس ماندن، امکان خیال‌پردازی و تنوع گوناگون محیط‌های اینترنتی، فرصت مناسبی را برای بروز خلاقیت فراهم می‌کند.

مبانی و چارچوب نظری پژوهش

فضای مجازی (سایبری)

واژه‌ی سایبر از لغت یونانی Kybernetes به‌معنی سکاندار یا راهنما مشتق شده است. نخستین بار این اصطلاح «سایبرنتیک» توسط ریاضیدانی به‌نام «نوربرت وینر» در کتابی با عنوان «سایبرنتیک و واپایش در ارتباط بین حیوان و ماشین» در سال ۱۹۴۸ به‌کار برده شده است. سایبرنتیک علم مطالعه و واپایش مکانیزم‌ها در سامانه‌های انسانی، ماشینی (و رایانه‌ها) است.

سایبر پیشوندی است برای توصیف یک شخص، یک شئی، یک ایده و یا یک فضا که مربوط به دنیای رایانه و اطلاعات است.

فضای مجازی(سایبر) در معنا به مجموعه‌هایی از ارتباطات درونی انسان‌ها از طریق رایانه و وسایل مخابراتی بدون در نظر گرفتن جغرافیای فیزیکی گفته می‌شود.

وقتی صحبت از فضای مجازی به میان می‌آید مردم اغلب به رایانه‌هایی فکر می‌کنند که به اینترنت متصل است؛ در حالی‌که این فقط بخش بسیار کوچکی از فضای سایبر را تشکیل می‌دهد. از نگاه «دیویدبل» (۲۰۰۱) فضای مجازی فقط مجموعه‌ای از سخت‌افزار نیست بلکه مجموعه‌ای از تعاریف نمادین است که شبکه‌ای از عقاید و باورها را در قالب دادوستد بیت ردوبدل می‌کنند.

فضای مجازی در واقع نامی است که تعداد زیادی از کاربردهای امروز فناوری‌های جدید ارتباطی را دربر می‌گیرد. این نام نخستین بار به‌وسیله‌ی «ویلیام گیبسون» در رمان «نورومانسر» ابداع شد (هولمز، ۲۰۰۵). همان‌طورکه «کاترین هایلس» (۱۹۹٦) نشان می‌دهد دیدگاه «گیبسون» خودبه‌خود به‌وجود نیامده بود و دگرگونی‌های مبتنی بر فناوری انجام شده در دهه‌های ۱۹۸۰ و ۱۹۹۰ نقش زیادی در ظهور این اصطلاح داشت. ظهور فضای مجازی در واقع درست بعد از پایان جنگ جهانی دوم و با راه افتادن موج فناوری‌های جدید رایانه‌ای در فرم اولیه آن اتفاق افتاد (دهقان، ۱۳۸٤).

فضای مجازی یک شبکه‌ی گسترده‌ی جهانی است که شبکه‌های مختلف رایانه‌ای در اندازه‌های متعدد و حتی رایانه‌های شخصی را با استفاده از سخت‌افزارها و نرم‌افزارهای گوناگون و با قراردادهای ارتباطی به یکدیگر وصل می‌کند. فناوری‌های ارتباط راه دور، اساس فضای مجازی را تشکیل می‌دهند (ویتاکر ,۲۰۰٤) هر چند برخی از این فناوری‌ها مانند تلگراف و تلفن در اوایل قرن نوزدهم اختراع شده بودند اما همه‌گیر و ارزان شدن این فناوری‌ها و بالارفتن توان فنی آنها که شرط اصلی ظهور فضای مجازی است در چند سال اخیر اتفاق افتاده است. «ویتاکر» در

توضیح این مسئله به رویداد تاج‌گذاری ملکه‌ی انگلستان اشاره می‌کند که حدود بیست میلیون نفر آن را از تلویزیون تماشا کردند. در حالی‌که تعداد تلویزیون‌ها در انگلستان تا قبل از چند ماه مانده به مراسم ٦٠٠٠٠٠ دستگاه برآورد می‌شد اما در طول چند ماه، این تعداد تلویزیون در انگلستان خریداری شد. شیوع فناوری‌های ارتباطی در سال‌های بعد کم‌کم به شکل‌گیری و ظهور فضای مجازی منجر شد.

کلمه‌ی فضای مجازی (سایبر اسپیس) از درون کلمه سایبرنتیکس که در سال ١٩٤٨ به‌وسیله‌ی «نوربرت وینر» ابداع شده بود پدید آمد. سایبرنتیکس علم نظریه‌ی واپایش است و در مورد سامانه‌های پیچیده به‌کار می‌رود (ویتاکر، ٢٠٠٤). تمام سامانه‌هایی که با روش‌های خودفرمایی اداره می‌شوند در واقع سامانه‌های سایبرنتیکی هستند. گاهی کلمه‌ی سایبرنتیکس در معنایی غیر از معنای اولیه آن؛ به‌طور مثال: به معنای قانون‌گذاری و قانونمندی به‌کار می‌رود (دامسایر ١٩٩٣ و بیر ١٩٩٤). دلیل این نوع نام‌گذاری به پیچیدگی این نوع قوانین مربوط می‌شود. ارتباط واژه‌ای فضای مجازی (سایبراسپیس) و سایبرنتیکس هم به مسئله‌ی پیچیدگی برمی‌گردد.

نقش ضداطلاعات در حفاظت اطلاعات

ضداطلاعات را فعالیت‌های طراحی شده برای حفاظت از اطلاعات طبقه‌بندی شده یا حساس، عملیات اطلاعاتی، فناوری‌های نظامی و فعالیت‌های دیپلماتیک مربوط به مسائل امنیت ملی تعریف می‌کنند.

ضداطلاعات نقش مهمی در همه‌ی برنامه‌های اثربخش سازمان دارد. این نقش شامل ارائه‌ی ارزیابی‌هایی از توانمندی‌های دشمن در زمینه‌ی جمع‌آوری اطلاعات و تهدیدهای بالقوه‌ی طرف‌های ذینفع خارجی، همکاری نزدیک با کارشناسان فنی برای شناسایی آسیب‌پذیری‌های نظام‌مند و توصیه‌ی تدابیر مناسب برای کاهش خطر و تأمین پشتیبانی ضداطلاعاتی از برنامه‌های آموزش و یاددهی می‌شود. کارشناسان ضداطلاعات باید شانه‌به‌شانه‌ی کارشناسان فنی، مدیران حفاظتی مدیران شبکه، برای طراحی سیاست‌ها و رویه‌های ایمن‌سازی اطلاعات حساس در محل کار

فعالیت کنند. این فعالیت‌ها عبارتند از :

- انجام تحقیقات کارکنان، بررسی سوابق و مجوزدهی به کارکنانی که باید به سامانه‌های حساس اطلاعات- فناوری، برنامه‌های طبقه‌بندی شده و اطلاعات حساس دسترسی داشته باشند
- انجام ارزیابی‌هایی درباره‌ی توانمندی‌های خاص دشمن علیه سامانه‌های اطلاعاتی و مخابراتی
- کمک به متخصصان فناوری اطلاعات به‌واسطه‌ی تأمین اطلاعات تهدید و ارزیابی آسیب‌پذیری
- ارائه‌ی توصیه‌هایی درباره‌ی توسعه‌ی سامانه‌ها، دستورکارها و سیاست‌های طبقه‌بندی شده
- کمک به متخصصان فناوری اطلاعات به‌واسطه‌ی رویه‌های ممیزی سامانه‌ها و نظارت رفتاری بر فعالیت شبکه
- ارائه‌ی توصیه‌ها و آموزش‌هایی به کارکنان درباره‌ی رویه‌های امنیت اطلاعات، تهدیدهای بالقوه و آسیب‌پذیری‌های سامانه‌ها و عملیات
- هماهنگی با کارشناسان فناوری اطلاعات برای برنامه‌ریزی پاسخ به حوادث
- هماهنگی با تیم حفاظت اطلاعات برای انجام مشترک تحقیقات پس از حادثه درباره‌ی نفوذ به شبکه‌ها، حوادث مشکوک به جاسوسی مجازی یا هرگونه افشای اطلاعات حساس
- ارائه‌ی توصیه‌هایی به مدیران شبکه و کارکنان حفاظت اطلاعات درباره‌ی تدابیر مقابله‌ای و کاهش آسیب‌پذیری‌های سامانه

شناسایی تهدیدهای بالقوه کارکنان در فضای مجازی

جاسوسی مجازی، تهدید ضد اطلاعاتی خاصی است؛ چرا که دشمن به‌واسطه‌ی آن، پیوسته حضور دارد اما تشخیص آن و حتی اینکه اتفاقی در حال وقوع است دشوار است. از این گذشته، کارکنان خبره‌ی غیرفنی، اغلب با فنون زیرپاکشی مجازی یا نحوه‌ی اثرگذاری بالقوه کنش‌های فرد بر امنیت کل شبکه ناآشنا هستند. هرچند شاید واقع‌گرایانه نباشد که انتظار داشته باشیم همه‌ی کارکنان درکی پیشرفته از

امنیت شبکه داشته باشند اما آموزش ابتـدایی فنـون رایـج بهـره‌بـرداری مجـازی در شناسایی موارد بالقوه‌ی زیرپاکشی سودمند است.

جاسوسی مجازی بیشتر با بهره‌برداری دشمنان از آسیب‌پذیری‌های زاییده‌ی رفتـار انسانی و نه نقص فنی، آغاز می‌شـود. اطلاعـات مربـوط بـه هـدف را از اطلاعـات حوزه‌ی عمومی، اینترنت یا دیگر منـابع بـاز، گـردآوری مـی‌کننـد تـا فرصـت‌هـای بهره‌برداری را تشـخیص دهنـد. مراحـل اولیـه‌ی حملـه‌ی مجـازی مشـابه عملیـات اطلاعات انسانی است. نخست، شناسـایی هـدف‌هـای بـالقوه‌ای کـه گمـان مـی‌رود موقعیت و دسترسی مناسبی داشته باشند و بعـد ارزیـابی آنهـا از طریـق جمـع‌آوری اطلاعات و با استفاده از اطلاعات در دسـترس عمـوم مثـل: شـبکه‌هـای اجتمـاعی، اطلاعات پروژه و دیگر اقلام قابل دسترسی آنلاین، حالا مهاجمان از ایـن اطلاعـات برای طراحی شگردهای دشوار و از نظر اجتماعی مهندسی شده استفاده می‌کننـد تـا مقدمات وارد کردن بدافزار را برای حمله‌ی مورد نظر فراهم کنند.

شگردها، اغلب در قالب نامه‌های الکترونیکی است که به‌ظاهر از طـرف همکـاران یا دیگر افراد مشروع آمده است، عملی می‌شوند یا در قالب حمله‌های فیشینگ که از طریق اغواگری‌های حساب شده‌ی اجتماعی، قربانی را به وب‌گاه‌هـا مـی‌کشـانند تـا مجوزهای دسترسی، اطلاعات شخصی و... را بدزدند.

مطالعات انجام شده حاکی از آن است که بخـش عمـده‌ی ایـن نـوع حملـه‌هـای هدفمند از چند کشور چین (۲۸/۲ درصد)، رومانی (۲۱/۱ درصد) و امریکا (۱۳/۸درصد) ریشه می‌گیرند و افرادی که بیش از همه هدف قرار گرفته‌اند هم شـامل کارشناسـان سیاست دفاعی، هیئت‌های دیپلماتیک و پژوهشگران بوده‌اند.

رایج‌ترین تهدیدهای اطلاعات دیجیتالی مجازی شامل موارد زیر است:

- از دست رفتن یا سرقت تجهیزات
- حقه‌های مهندسی اجتماعی
- بدافزار
- دسترسی غیرمجاز به سامانه‌ها
- خطای کاربر

پرهیز از زیر پاکشی مجازی

آسان‌ترین راه برای پرهیز از قرار گرفتن در معرض حمله‌های هدفمند، داشتن نمایه‌ی دیجیتالی کم‌نماست. پایبندی به چند دستورکار ابتدایی حفاظتی، نقش مهمی در ایمن کردن اطلاعات و شبکه‌ها از نفوذ دارد. مطمئن شوید که کارکنان، اسناد کاری را به رایانه‌های خانگی یا قابل حملشان پست الکترونیکی نمی‌کنند؛ مراقب ویروس‌ها و اسب ترواییی که دشمن اغلب از آنها برای نقشه‌برداری، بهره‌برداری و کنکاش سامانه‌های شبکه‌ای استفاده می‌کند، باشید و بر استفاده از حافظه‌ها و ابزارهای رسانه‌ای قابل حمل که از ابزارهای اصلی دسترسی منابع تهدید به سامانه‌های شبکه‌ای هستند نظارت کنید.

دستگاه‌های اطلاعاتی خارجی و متخصصان اطلاعات رقابتی فعالانه در اتاق‌های گپ، انجمن‌های گفت‌وگو، گروه‌های خبری و شبکه‌های اجتماعی، به‌دنبال اطلاعات، منابع و ارتباطات هستند. کارکنانی با مناصب حساس یا دسترسی به اقلام دارای طبقه‌بندی، نباید اطلاعات حرفه‌ای را در شبکه‌های اجتماعی منتشر کنند. جزئیاتی مثل محل کار، سازمان، پروژه‌ها، مجوزهای امنیتی، اطلاعات تماس، پست الکترونیکی، شماره‌های تلفن و دیگر داده‌های شخصی هرگز نباید در شبکه‌های اجتماعی در دسترس همه باشند. از این گذشته، اطلاعات شخصی را اغلب به آسانی می‌توان به جایگاه حرفه‌ای، پروژه‌ها یا محل کار ارتباط داد و کارکنان هرگز نباید در فضای مجازی بگویند که به اطلاعات حساس یا طبقه‌بندی شده دسترسی دارند.

یکی از راه‌های مهم برای حفاظت از اطلاعات حساس موجود در سامانه‌های منفرد یا شبکه‌ای، اجتناب از فنون رایج زیرپاکشی مورد استفاده‌ی جمع‌آوری کنندگانی است که می‌کوشند به اطلاعات دسترسی یابند. همه‌ی کارکنان باید از قواعد سرانگشتی زیر مطلع باشند تا از ایمنی اطلاعات دیجیتالشان اطمینان یابند:

- به نامه‌های الکترونیکی ناشناسی که اطلاعات شخصی از شما می‌خواهند جواب ندهید.
- اطلاعات مالی خود را به کسی ندهید.

- از نرم‌افزارهای ضدویروس و ضدجاسوسی استفاده کنید.
- از منبع تماس‌های تلفنی یا نامه‌های الکترونیکی درخواست نشده " مراکز پشتیبانی" که برای حل مشکلات شبکه، پست الکترونیکی یا سامانه‌ها پیشنهاد کمک می‌دهند مطمئن شوید.
- دیواره‌های آتشین یا نرم‌افزارهای امنیتی تعبیه شده توسط مدیر سامانه را دور نزنید و نادیده نگیرید.
- مراقب نامه‌های الکترونیکی با نشانی‌های ناآشنا یا کشورهای خارجی باشید.
- از نامه‌های الکترونیکی نامعلومی که به‌ظاهر از یکی از حساب‌های کاربری داخلی سازمانی می‌آیند، مطمئن شوید.
- مراقب نامه‌های الکترونیکی شخصی فرستنده‌های ناشناس باشید.
- مراقب فرستنده‌ی ناشناسی که خود را دانشجو یا مشاور معرفی می‌کند، باشید.
- مراقب فرستنده‌ای که نماینده‌ی دولتی خارجی است یا ادعا می‌کند به نمایندگی از دولتی خارجی فعالیت می‌کند، باشید.
- مراقب فرستنده‌ی ناشناسی که ادعا می‌کند از کار در برنامه‌های طبقه‌بندی شده یا پروژه‌های حساس " مرخصش کرده‌اند" باشید.
- مراقب فرستنده‌هایی که درباره‌ی پروژه‌های مرتبط با فناوری دفاعی پرس‌وجو می‌کنند باشید؛ به‌خصوص اگر شناختی چشمگیر از برنامه، فناوری یا سامانه‌ای خاص دارند.

توصیه‌های امنیتی برای استفاده ایمن از رایانه‌های همراه و تلفن همراه

با توجه به چندکاره بودن ابزارهای همراه امروزی، از دست رفتن این ابزارها می‌تواند به سرقت داده‌های ذخیره شده، شنود ارتباطات، تعقیب موقعیتی و بهره‌برداری از اطلاعات، داده‌های شخصی و شبکه‌های اجتماعی کاربر که ممکن است اطلاعاتی زمینه‌ای برای حمله‌های دشوارتر فراهم کنند، منجر شود. به‌علاوه لپ‌تاپ‌ها و گوشی‌های همراه، به‌دلیل ماهیت کاربردشان، به‌واسطه‌ی

همسان‌سازی اطلاعات و دیگر ارتباطات، اغلب سکوی اولیه‌ی ورود ناخواسته‌ی بدافزارهای فاسد به رایانه‌های میزی و سامانه‌های شبکه‌ای می‌شوند.

هر چند ابزارهای همراه، جزء جدایی‌ناپذیر کسب‌وکار شده‌اند، این ابزارها آسیب‌پذیری‌های ذاتی با خود دارند که دلیل اصلیش برخورداری سامانه‌های شبکه‌ای ثابت از واپایش‌های امنیت فیزیکی و حفاظت‌های مستحکم‌تر فنی است. مزایای ابزارهای همراه (حمل‌پذیری و اتصال پیوسته) هم احتمال سرقت یا از دست رفتن این ابزارها را بیشتر می‌کنند.

کارکنان همچنین باید از آسیب‌پذیری‌ها و خطرهای ضداطلاعاتی به‌خصوص هنگام سفر به مناطق پرخطر مطلع باشند. این آسیب‌پذیری‌ها شامل موارد زیر است:

- شنود الکترونیکی تماس‌های تلفنی، پیامک‌ها و نامه‌های الکترونیکی
- از دست رفتن اطلاعات به‌دلیل سرقت ابزار یا دستکاری پنهانی سخت‌افزار
- تعقیب موقعیتی از طریق ابزارهای متصل به شبکه‌ی تلفن (GPS)
- تلاش‌های فیشینگ و هرزنامه از حاملان شبکه‌های خارجی
- دریافت پوشه‌های رسانه‌ای آلوده یا بدافزارها به‌واسطه‌ی پیام‌رسانی یا ارتباط بلوتوثی

سیاست امنیتی ابزارهای همراه، حداقل باید شامل قواعدی اساسی برای استفاده‌ی ایمن و دستورکارهای رفتاری، آگاه‌سازی از تهدیدها، آموزش تدابیر مقابله‌ای، حفاظت‌های فنی و رویه‌های مدیریت استاندارد خطر باشد. به‌علاوه مدیران سامانه‌ها و کارکنان حفاظتی و ضداطلاعاتی باید دستورکاری برای اقدام فوری در صورت از دست رفتن، سرقت یا گم شدن ابزارهای همراه یا در شرایطی که کاربر به شنود، اختلال یا دستکاری وسیله‌اش ظنین است در اختیار کارکنان بگذارند. مدیران امنیتی همچنین باید دستورکارهای روشنی درباره‌ی استفاده از رایانه‌های همراه و ابزارهای همراه شخصی در سفرهای رسمی تدوین کنند. به‌دلیل آسیب‌پذیری‌های منحصر به فرد این ابزارها، کارکنان هرگز نباید از رایانه‌های همراه یا ابزارهای همراه شخصی تأیید نشده برای پردازش، ذخیره یا انتقال اطلاعات حساس مربوط به کار استفاده کنند.

حفاظت از اطلاعات منابع آشکار در وب

با همه‌ی نگرانی‌ها درباره‌ی عوامل نفوذی، فعالیت‌های پنهانی، نظارت فنی پیشرفته و حمله به شبکه‌های رایانه‌ای، شاید پرثمرترین ابزار جمع‌آوری اطلاعات تشکیلات خارجی، هم‌چنان دسترسی قانونی به داده‌های منابع آشکار و بهره‌برداری از اطلاعات آشکار حفاظت نشده باشد. در جامعه‌ی جهانی، جمع‌آورندگان خارجی می‌توانند بدون متوسل شدن به ابزارهای غیرقانونی و فعالیت‌های محرمانه، گنجینه‌ای از اطلاعات ارزشمند به‌دست آورند؛ حتی اطلاعات طبقه‌بندی نشده‌ای که به ظاهر ارزش اطلاعاتی چشمگیری ندارند، می‌توانند عناصری مهم برای جمع‌آورندگان خارجی باشند. چنین اطلاعاتی می‌توانند شکاف‌های داده‌های موجود را پر کنند، به یافتن و ارزیابی منابع کمک کنند و برای شناسایی هدف‌های بالقوه و روش‌های جمع‌آوری اطلاعات سودمند باشند. بارها پیش می‌آید که جمع‌آورندگان اطلاعاتی، از فنون داده‌کاوی و نظارت بر وب‌گاه‌ها، اتاق‌های گپ، خبرنامه‌های الکترونیکی و مطالب عمومی برای جست‌وجوی هدف‌های مطلوب و شناسایی افراد مطلعی که به اطلاعات دسترسی دارند، استفاده کنند.

مدیران ضداطلاعاتی و امنیتی باید از دامنه‌ی وسیع اطلاعات عمومی در دسترس گردآورندگان خبره و مصمم آگاه باشند؛ هرچند این اطلاعات، به خودی خود، بی‌ضرر به‌نظر می‌رسند، در کنار دیگر اطلاعات هدف‌گیری شده‌ی گردآورندگان خارجی، می‌توانند دارایی‌هایی با ارزش‌تر را به‌خطر بیندازند.

بخشی از ارزیابی آسیب‌پذیری سازمانی، باید انواع اطلاعات سازمانی در دسترس ناظران بیرونی را بررسی کند و سطح مناسب خطرپذیری ناشی از در دسترس بودن این اطلاعات را تعیین کند. بعد بایستی برای قاعده‌مند کردن اطلاعاتی که می‌توان در وب‌گاه منتشر کرد، نحوه‌ی بازبینی آنها و چگونگی واپایش یا نظارت بر دسترسی بیرونی را توسعه داد.

اینکه اطلاعاتی طبقه‌بندی نشده است بدین معنی نیست که قرار دادنش در معرض دسترسی‌های واپایش نشده یا در درگاه‌های رمزگذاری نشده‌ی اینترنتی درست است. سازمان‌ها به‌عنوان بخشی از برنامه‌های امنیتی و ضدعملیاتی خود باید

سیاستی برای تعیین مطالبی که می‌توان آنها را برای مصرف عموم در اینترنت منتشر کرد تدوین کنند. بعضی از این عوامل موارد زیر هستند :

- مخاطب هدف کیست؟ آیا این اطلاعات برای مشتریان یا افکار عمومی ضروری هستند؟
- تهدیدهای بالقوه برای این اطلاعات چه هستند؟ چه کسی احتمال دارد به آنها دسترسی داشته باشد؟
- آیا این اطلاعات را می‌توان با دیگر داده‌های منابع آشکار تلفیق کرد تا به پیوندها و ارتباطاتش با داده‌های حساس‌تر دیگر پی برد؟
- آیا واپایش‌ها و نظارت‌های امنیتی مناسبی بر مطالب منتشر شده در وب‌گاه حاکم هستند؟

هر سازمان باید فهرستی اختصاصی از مطالبی که انتشار اینترنتی آنها پذیرفتنی است تهیه کند. در بعضی موارد، اطلاعات داخلی به ظاهر بی‌ضرر، می‌توانند شناخت ارزشمندی به بیرونی‌ها بدهند؛ حتی مواردی مثل: خبرنامه‌ها، گزارش‌های مطبوعاتی و نشریه‌های داخلی هم می‌توانند اطلاعات حساسی را افشا کنند و باید پیش از انتشار، آنها را بازبینی کرد.

نتیجه‌گیری

ضداطلاعات موضوعی چندرشته‌ای است و نباید آن را تنها یکی از وظایف مدیران سامانه‌ها و کارشناسان فناوری فرض کرد. یک برنامه‌ی اثربخش امنیت اطلاعات مستلزم تلاش‌های همکاران و متخصصان ضداطلاعات و حفاظت فیزیکی و... است و کارکنان حداقل چند مؤلفه اساسی زیر را باید رعایت کنند:

۱. قواعد مناسب برای تعیین، متمایزسازی، ذخیره، انتقال و نابودی اطلاعات حساس
۲. قواعد و رویه‌های استفاده‌ی مناسب از سامانه‌ها و شبکه‌های اطلاعاتی
۳. دستورکارهای استفاده‌ی ایمن از تلفن همراه و وسایل بی‌سیم
٤. تشخیص و واکنش به تهدیدهای مجازی و رخنه‌های شبکه‌ای

۵. استفاده‌ی ایمن از ابزارهای ذخیره‌ی رسانه‌ای دیجیتال
٦. رویه‌های تأیید انتشار عمومی اطلاعات و حفاظت از اطلاعات منابع آشکار در فضای مجازی
۷. آگاهی از تهدیدها و آسیب‌پذیری‌های فضای مجازی
۸. پرهیز از زیرپاکشی مجازی و استفاده از تدابیر مقابله‌ای برای حفاظت از منابع اطلاعاتی در فضای مجازی

منابع و مآخذ

- ابری، انسیه (۱۳۸۷)، «**فضای مجازی عرصه ظهور خلاقیت**»، اولین کنفرانس ملی خلاقیت‌شناسی مهندسی و مدیریت نوآوری ایران.
- اکبری، ابوالقاسم؛ اکبری، مینا (۱۳۹۰)، «**آسیب‌شناسی اجتماعی**»، تهران: انتشارات رشد و توسعه.
- افتخاری، اصغر (۱۳۹۰)، «**راهبرد ملی برای تأمین امنیت در فضای مجازی**»، تهران : پژوهشکده مطالعات راهبردی.
- احمدوند، علی محمد، عطایی، امیر مسعود (۱۳۸۹)، «**نقش و راهبرد فناوری اطلاعات در سامانه‌های پلیس و فضاهای مجازی در ایران**»، دو ماهنامه توسعه انسانی پلیس، سال اول، شماره ۳.
- آویکا، دیوید جی (۱۳۸۳)، «**راه‌کارهای پیشگیری و مقابله با جرایم رایانه‌ای**»، ترجمه‌ی اکبر استرکی؛ محمد صادق روزبهانی، تهران: معاونت پژوهش دانشگاه علوم انتظامی امین.
- آشوری، محمد (۱۳۸٦)، «**مقدمه‌ای بر کتاب جرایم رایانه‌ای**»؛ چاپ دوم، انتشارات بهنام.
- یاسمی‌نژاد، عرفان؛ آزادی، اکرم؛ امویی، محمدرضا (۱۳۹۱)، «**فضای مجازی، امنیت اجتماعی و راهبردها**»، همایش ملی صنایع فرهنگی نقش آن در توسعه‌ی پایدار.
- The Economic Espionage Act criminalizeds trade secrets misappropriation .U.S.C
- Securing Cyberspace for the ۴۴th Presidency. Center for Strategic and international Studies Commission on Cybersecurity for the ۴۴th Presidency. Washington D.C December ۲۰۱۱.
- Trends in Proprietary Information Loss, ASIS Foundation Report(۲۰۱۰)
- U.S . China Economic and Security Review Commission,۵۱
- Mike McConcell, How to Win the Cyber-war Washington post,February ۲۸,۲۰۱۰,page ۱۰
- Cyberspace Policy Review,Assuring a Trusted and Resilinet information, May ۲۰۰۹
- Shadows in the cloud: Investigation Cyber Espionage information warfare monitor April ۲۰۱۱
- Twenty Critial Control for effective cyber defence . November ۲۰۱۳