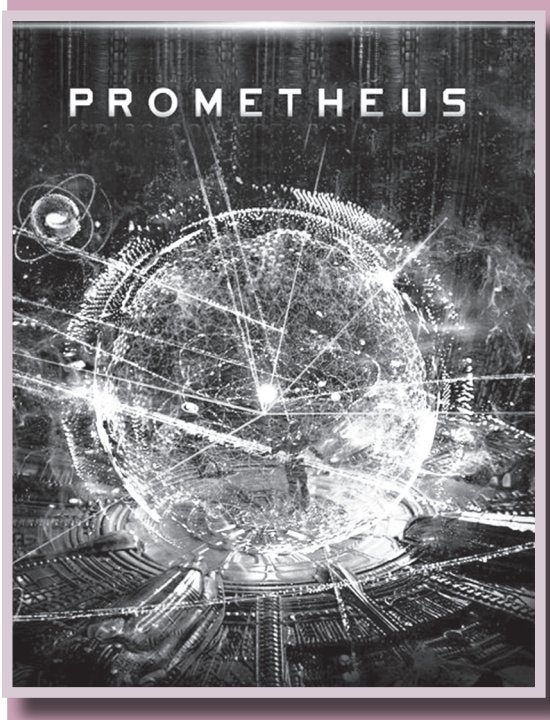
افسانه پرومته در عصر دیجیتال



P.B. Usieto

من از خردسالی به داستانهایی علاقه‌مند بودم که سرپیچی انسانها از خدایان و آفریدگان را با استفاده از اختراع فناوری روایت می‌کرد و بهای عواقب هولناکی که آنها بابت کنجکاویشان باید می‌پرداختند، تخیل مرا بیشتر جذب می‌کرد.

داستان اساطیری پرومته که به‌رغم فرمان زئوس، برای انسانها آتش فراهم می‌کند، اولین عاقبت منفی را برای بشریت به‌همراه داشت: جعبه پر از بیماری و رنجِ **پاندورا**[1]. البته با وجود اینکه چنین **کابوس‌آبادی**[2] در آینده و به این شکل فجیع (دست‌کم در کوتاه‌مدت) روی نخواهد داد، اما در رابطه با حریم خصوصی و امنیت سایبری، خطرهای واقعی وجود دارند؛ به‌رغم هشدارهایی که طی سالهای قبل نیز داده شده و معنای واقعی آنها را هنوز به خوبی درک نکرده‌ایم. این خطرها تنها شرکتها و مؤسسه‌های عمومی را تحت تأثیر قرار نمی‌دهد، بلکه بر زندگی ما نیز به‌طور مستقیم اثر خواهد گذاشت.

صفحه شطرنج جدید

نفوذ فناوری به تمامی ابعاد زندگی، شهرها و بدن انسان را به سامانه اطلاعاتی تبدیل کرده که داده‌ها را به‌وسیله گروه وسیعی از دستگاه‌های مجهز به حسگرهای نظارت ۲۴ساعته، تولید، پردازش و انتقال می‌دهد و قابلیت تعامل با هر نوع رابط قابل‌تصور، آناتومیک و حتی شناختی را دارد. امروز، بازارهای متمرکز بر یک محصول خاص،

محصولاتـی ماننـد رباتهای نگهـداری از افـراد کم‌توان، کاشـتنیهای پزشـکی، یا دسـتگاه‌های رایانـه‌ای رابط مغز را عرضه می‌کنند که در سـالهای آینده بهینه‌سـازی شـده و به‌احتمال بـه تولید انبوه نیز خواهند رسـید. البته پیامدهای حمله‌های سایبری به این محصولات، مشابه موارد دیگری نیست که امروز در اخبار شاهدشـان هستیم. نفوذ به سامانه یک ربات مجهز به فناوری پیشرفته و دارای کنترل در سامانه هوشـمند خانگی یا رخنه در کامپیوتر خدمت‌رسان تجهیزات پزشکی مربوط به مرگ و زندگی انسان، با حمله باج‌خواهانه به رایانه‌های شـخصی قابل‌مقایسه نیسـت. حتی با فرض اینکه به‌دلیل تعداد کم کاربران این دستگاه‌ها، این سناریوها بعید باشـند، با پیش‌بینی افزایش میلیاردها دسـتگاه متصل به‌هـم در فناوری **اینترنت اشیا**[۳] تا سـال ۲۰۲۰، به‌احتمال زیـاد انگیزه بـرای جرم و جنایت سـازمان‌یافته و سـودآور به‌وسیله افراد ناشناخته فراهم می‌شود.

به‌طور کلی، پیامدهـای حریم خصوصی مرتبط با خدمات آینـده، ماهیـت متفاوتـی خواهد داشـت. نـوع داده‌های ایجادشده به‌وسیله حسـگرهای نظارت ۲۴ساعته، به‌مراتب بیشتر و بیشـتر در زندگی خصوصی وارد خواهد شد؛ چرا که این داده‌ها با طول عمر، وضعیت بیماریها، نحوه تفکر و حتی عملکرد ما در محل کار سروکار دارند.

در اختیار داشـتن ایـن حجم داده، قدرت بیشـتری برای مالکان آن به‌وجود می‌آورد که شـرح حال دقیق اشخاص را تهیه می‌کنند و چنین اطلاعاتی، آماده فروش به مشـتریان مورد نظر از جمله شـرکتهای بیمه، بانکها، شرکتهای منابع انسـانی یا دولتها است. دسترسی به سامانه خدمات درمانی، وام، شغل یا حتی تبلیغات، به شرح حال افراد و نزدیکی آنها بـه ممتازترین طبقه اجتماعی، بسـتگی خواهد داشـت. در آینـده، این موضوع پیامدهای نامطلوب برای افراد دارد؛ چرا که در قبل، این اطلاعات در دسترس نبوده است.

راهبردهایی برای نمایشنامه‌های آینده

این تغییـر الگو باید به‌طور کامل برای صنعت امنیت سـایبری شـفاف باشـد. پاسـخ باید جهانی بوده و رویکـرد باید به‌طور اساسی تغییر کند.

اگـر راهکارهای فعلـی امنیت سـایبری در کاهش حملات موجود ناتوان باشـند و تغییرهای لازم را ایجـاد نکنند، با بدتر شدن برخی آمارها مانند کاهش تعداد افراد مستعد در حوزه امنیت سـایبری، آموزش ضعیف امنیت برای بیشتر کاربران نهایی، و نبود طراحی امنیتی در بیشـتر نرم‌افزارهـای کاربردی اینترنت اشـیا، این راه‌حلها به هیـچ دردی نخواهند خورد. متخصصان امنیت سـایبری بیش از هر زمان دیگری به خلاقیت نیاز دارند تا با شیوه‌ای متفاوت به مشکلات نگاه کرده و دیدگاه‌های جدید مطرح کنند.

در اینجا فهرسـتی از اقدامهایی می‌آید کـه پیرو این مفهوم هستند؛ حتی اگر هنوز مطمئن نباشیم که صددرصد امکان‌پذیر باشند:

- تمرکـز متخصصان امنیت سـایبری نمی‌تواند تنها بر فناوری

با پیش‌بینی افزایش میلیاردها دستگاه متصل به‌هم در فناوری اینترنت اشیا تا سال ۲۰۲۰ به احتمال زیاد انگیزه برای جرم و جنایت سازمان‌یافته و سودآور به‌وسیله افراد ناشناخته فراهم می‌شود

اطلاعـات و راهبری باشـد. درک ماهیت محصولات و خدمات جدید بـرای ارائه اقدامهای امنیتی مناسـب، ضروری اسـت. متخصصـان امنیت سـایبری جدیـد باید در رشـته‌هایی مانند شهرنشینی، آناتومی، زیست‌شناسی، علوم اعصاب و روانشناسی پدیدار شوند؛

• در عیـن حال، صنایع جدید نیازمنـد گنجاندن اقدامهای امنیتی در برنامه‌های خود هستند. بنابراین، باید موقعیتهای بیشـتری در زمینه امنیت سایبری به‌منظور کمک، آموزش و ارائه خدمات مشاوره‌ای به افرادی که متخصصان امنیتی نیسـتند، فراهم آید تا از پوشـش تمامی حوزه‌های امنیتی اطمینان کسب شود؛

• با استفاده از مزایای این محیط جدید، باید از رویکردهای تحلیلی متفاوتی برای کاهش هجومها استفاده کرد. مانند:

○ پیشـرفت در زمینه‌های دیگر (برای نمونه، هوش مصنوعی، رباتیک، علوم اعصاب)؛

○ تعداد زیاد دسـتگاه‌های متصل به یکدیگـر که نه‌تنها نباید به چشـم یک معضل دیده شوند، بلکه باید به‌عنوان شـبکه‌ای بزرگ از منابـع امنیتی شناسـایی گردند که در صورت نیاز، ممکن است به‌وسیله **مرکز عملیات امنیتی**[۴] استفاده شوند؛ و

○ اطلاعات تکامل‌یافته، حاصل هم‌افزایی بین بخشهای امنیت ملی سـایبری و تولیدکنندگان ابـزار امنیتی خواهد بود.

• کاربر نهایـی نمی‌تواند از خطرهای مربوط به امنیت و حریم خصوصی که به‌واسـطه فناوری به‌وجود می‌آیند، ناآگاه باشد. بـه همین دلیل، باید آموزش و آگاهـی درباره امنیت، مطابق با پیامدهای جدید اجرا شـود؛ امـا همان‌گونه که می‌دانیم، در بیشتر اوقات نقض امنیت رخ می‌دهد؛ زیرا با وجود آموزشها، کاربران توانایی اسـتفاده از اقدامهای امنیتی را ندارند. به این ترتیب، باید برای تأمین امنیت دسـتگاه‌ها روشهای جدیدی به‌وجود آوریم، برای نمونه، تغییر برخی مسئولیتها در صورتی که دسـتگاه خاصی به‌دلیل غفلت کاربر/ اسـتفاده‌کننده، مورد حمله قرار گیرد؛ و

• آخریـن مـورد که به انـدازه دیگر مـوارد مهم اسـت، درباره انجمنهـای حرفه‌ای فناوری اطلاعات اسـت که باید پیامدهای دیجیتال‌سازی زندگی را درک کنند؛ بسیاری از آنها آیین اخلاقی را با تمرکز بر شـرکتها تدوین کرده‌اند، اما نقـش کاربر نهایی را لحاظ نکرده‌اند. همین امر برای سـازمانهای اسـتانداردگذار نیز صدق می‌کند.

بنابراین ...

خبر خوب این اسـت کـه مانند افسـانه پرومته، مجبور نیسـتیم بهای کنجـکاوی را بپردازیم؛ گرچـه از عواقب و پیامدهای آن آگاهیم و می‌دانیم که هر سـال بدتر می‌شود. اما اگر در آینده، شطرنج جدید را درست بازی کنیم و قوانین را به‌سرعت یاد بگیریم، نباید نگرانی خاصی داشته باشیم. همانطـور که زندگی به ترکیبی از نظـام طبیعی و دیجیتال تبدیل می‌شود، امنیت سـایبری نیز باید به یک رشته کلی تبدیل گردیده و در قلمروهای جدید گسـترش یابد و تصور رویکردهای جدیدی را آموزش دهد که اقدامهای نوآورانه را به‌وجود می‌آورد.

در این حیطه، سـهم مشـارکت و کمک شما چه خواهد بود؟

پانوشتها:

۱- جعبه پاندورا؛ به روایت افسـانه‌های یونانـی، جعبه‌ای بود حاوی تمامی بلاها و شـوربختی‌های بشـریت؛ از جمله بیمـاری، مرگ و غیـره. پاندورا ایـن جعبه را از زئوس دریافت کرد تا به انسـانها هدیه دهد و سـفارش کند که هرگز آن را نگشـایند. ولی پاندورا، خود جعبه را گشـود و بلاهـا و شـوربختی‌ها از داخل آن سـرازیر و روی زمین پراکنـده شـد؛ زمینی که تا آن زمـان هیچ‌گونه مشـکل و بدبختی را نمی‌شـناخت. تنها امید در جعبه باقی ماند تا تسلای خاطر بشر باشد. امـروز، عبارت بازکردن جعبـه پاندورا، برای صحبـت درباره اعمال کوچک غیرصحیحی به کار می‌رود که در نهایت پیامدهای فاجعه‌باری به‌دنبال خواهد داشت.

2- Dystopian

3- Internet of Things (IoT)

4- Security Operation Center (SOC)

منبع:

Usieto P.B., **Prometheus in the Digital Era**, The Nexus, 2017