The Art of Defense

نوشته و گردآوری: رضا ارغند، مصطفی ثابتی

مقاله ای درباره "هنر دفاع سایبری" (The Art of Defense)

پیش گفتار

سان‌تزو، یک فیلسوف جنگ باستانی است که استراتژی‌های جنگی را در قالب کتاب "هنر جنگ" تدوین کرده است. در محیط دیجیتال دائماً در حال تغییر جنگ سایبری، برنامه‌ریزی دقیق امری حیاتی است. حکمت ماندگار سان تزو در "هنر جنگ" اساس فلسفی قدرتمندی برای دفاع سایبری مدرن فراهم می‌کند در این نوشتار، از اصول ایشون در قلمرو امنیت سایبری استفاده کرده ایم.

بخش اول: برنامه‌ریزی استراتژیک امنیتی (Strategic Security Planning)

شناخت میدان نبرد (دارایی‌های دیجیتال)

سان تزو می‌گوید: ***"اگر دشمن و خود را بشناسی، در صد نبرد شکست نخواهی خورد."*** این اصل در امنیت سایبری به معنای فهرست‌برداری کامل دارایی‌هاست:

- **فهرست جامع دارایی‌ها** : یک استراتژی دفاعی قوی با شناسایی دقیق تمام دارایی‌های سازمان آغاز می‌شود. بدون این شناخت، نمی‌توان "قلمرو" خود را محافظت کرد.
- **درک اهمیت دارایی‌ها** : سازمان‌ها باید بدانند کدام دارایی‌ها بحرانی هستند و چگونه با اهداف کلی کسب‌وکار ارتباط دارند - این همان "شناخت زمین و موقعیت‌های استراتژیک" در اندیشه سان تزو است.
- **چالش مدیریت دارایی‌ها** : در محیط‌های بزرگ شرکتی، حفظ فهرست دقیق و به‌روز دارایی‌ها دشوار است و نیازمند فرآیندهای مستمر و خودکار می‌باشد. سان تزو این چالش را با تأکید بر "آمادگی مداوم" پیش‌بینی کرده بود.

شناخت دشمن (تهدیدهای سایبری)

"شناختن دشمن" در محیط سایبری به معنای درک تکنیک‌های مهاجمان است:

- **تکنیک‌های سازگارپذیر** : تهدیدهای امروزی از روش‌های پیچیده برای فرار از تشخیص استفاده می‌کنند، مانند پنهان شدن در میان ترافیک مشروع یا استفاده از فایل‌های به ظاهر معتبر. سان تزو این را "فریب و استتار" می‌نامید.
- **تهدیدات پنهان** : مهاجمان اغلب با صبر و حوصله عمل می‌کنند، که یادآور اصل سان تزو است: ***"جنگ هنر فریب است."*** شناسایی این تهدیدات نیازمند هوشیاری مداوم است.

مثال عملی: یک سازمان مالی با فهرست‌برداری دقیق از سرورهای پردازش تراکنش‌های بانکی (دارایی‌های حیاتی) و طبقه‌بندی آنها براساس اهمیت، توانست منابع دفاعی خود را هوشمندانه متمرکز کند و حملات هدفمند علیه سیستم‌های پرداخت را شناسایی و خنثی نماید.

برنامه‌ریزی دفاعی

سان تزو تأکید می‌کند: ***"پیروزی در جنگ قبل از ورود به میدان نبرد تعیین می‌شود."*** این اصل در امنیت سایبری به صورت زیر نمود می‌یابد:

- **آگاهی موقعیتی** : همان‌طور که سان تزو بر اهمیت جاسوسان و دیده‌بانان تأکید می‌کرد، در امنیت سایبری نیز باید سیستم‌های تشخیص و پایش را از منابع متعدد یکپارچه کرد تا تصویری جامع از وضعیت امنیتی به دست آورد.
- **استراتژی پاسخ به حوادث** : سان تزو می‌گوید: ***"آب شکل ظرف خود را می‌گیرد."*** یک استراتژی دفاعی موفق باید انعطاف‌پذیر بوده و شامل دستورالعمل‌های روشن برای واکنش سریع به انواع مختلف حملات باشد.
- **اولویت‌بندی منابع** : سان تزو تأکید می‌کند که ***"نمی‌توان همه جا قوی بود"*** در امنیت سایبری نیز باید منابع محدود را بر محافظت از دارایی‌های بحرانی متمرکز کرد.

جمع‌بندی

برنامه‌ریزی استراتژیک امنیتی، هنر محافظت از دارایی‌های دیجیتال از طریق شناخت عمیق "میدان نبرد" (دارایی‌ها)، "دشمن" (تهدیدها) و "قابلیت‌های خود" (کنترل‌های امنیتی) است. این رویکرد جامع به سازمان‌ها اجازه می‌دهد تا با دیدگاهی استراتژیک، چابک و هوشمندانه به تهدیدات سایبری پاسخ دهند و انعطاف‌پذیری خود را در برابر حملات تضمین کنند.

همان‌طور که سان تزو می‌گوید: ***"استراتژیست برتر آن است که بدون جنگ پیروز می‌شود."*** هدف نهایی برنامه‌ریزی استراتژیک امنیتی نیز همین است: ایجاد چنان دفاع قدرتمندی که مهاجمان را از حمله منصرف سازد.

بخش دوم: عملیات سایبری مؤثر (Effective Cyber Operations)

مقدمه

در حوزه دفاع سایبری، تنها رعایت چارچوب‌های انطباق هدف نهایی نیست؛ بلکه هدف اصلی متوقف کردن حملات و کاهش خطرات است. این امر مستلزم اقدامات قاطع و هوشمندانه است.

اصول سان تزو در عملیات سایبری مؤثر

سان تزو در فصل "جنگیدن" از کتاب هنر جنگ، اصلی بنیادین را مطرح می‌کند: ***"هدف جنگیدن، پیروزی است، نه صرفاً درگیر شدن در نبرد."*** این اصل در دفاع سایبری به این معناست که دفاع کنندگان باید بر کشف سریع تهدیدات، پیشگیری از حملات و کاهش تأثیر مخرب آنها تمرکز کنند.

سرعت و چابکی در دفاع

سان تزو می‌گوید: ***"سرعت، جوهره جنگ است."*** این اصل در دنیای سایبری اهمیت دوچندان دارد:

- **واقعیت سرعت حملات** : مهاجمان امروزی با سرعت شگرفی در اقدامات شان، عمل می‌کنند و گاهی تنها چند ثانیه برای نفوذ به شبکه و گسترش به سیستم‌های متصل زمان نیاز دارند.
- **لزوم واکنش سریع** : دفاع کنندگان باید بتوانند به سرعت تهدیدات را تشخیص داده، مشاهده کرده و پاسخ‌های خود را برای مختل کردن عملیات مهاجمان هدایت کنند.

مثال عملی: یک شرکت خدمات مالی با پیاده‌سازی سیستم تشخیص نفوذ خودکار توانست یک حمله باج‌افزاری را در مراحل اولیه شناسایی کند. با اقدام سریع و قطع دسترسی سیستم‌های آلوده از شبکه اصلی، از گسترش آلودگی و خسارت‌های گسترده جلوگیری شد.

آگاهی موقعیتی کامل

سان تزو می‌گوید: ***"اگر دشمن را بشناسی و خود را بشناسی، در صد نبرد خطری متوجه تو نخواهد بود."*** این اصل در عملیات سایبری به معنای داشتن آگاهی کامل از وضعیت است:

- **مشاهده خط زمانی حمله** : توانایی مشاهده و درک خط زمانی حمله و نحوه تخصیص منابع توسط مهاجمان، به دفاع کنندگان امکان می‌دهد تا اقدامات قاطع برای کاهش و رفع فوری حمله انجام دهند.
- **چالش تخصیص منابع** : اقدامات امنیتی ناکارآمد منابع سازمانی را هدر می‌دهند. محافظان باید بتوانند منابع خود را بهینه‌سازی کنند تا هزینه‌های نظارت امنیتی و پاسخ به حوادث را کاهش دهند.

اطلاعات تهدید و هوش مصنوعی

سان تزو بر اهمیت جاسوسان و اطلاعات پیش از نبرد تأکید می‌کند. در دنیای مدرن، این به معنای:

- **بهره‌گیری از اطلاعات تهدید** : دسترسی به اطلاعات دقیق درباره تاکتیک‌ها، تکنیک‌ها و روش‌های مهاجمان (TTPs) و بینش‌های حیاتی در مورد اهداف و انگیزه‌های آنها به دفاع کنندگان مزیت استراتژیک می‌دهد.

- **درک عمیق حملات پیچیده** : توانایی درک روابط متقابل که نشانگر تهدیدات اخلالگر هستند برای پیشگیری از تهدیدات و درک تکنیک‌های پیچیده مورد استفاده مهاجمان حیاتی است.

خودکارسازی و انعطاف‌پذیری

سان تزو می‌گوید: ***"لشکر باید مانند مار باشد... وقتی ضربه به سر وارد می‌شود، دم به کمک می‌آید؛ وقتی ضربه به دم وارد می‌شود، سر به کمک می‌آید."*** این اصل در دفاع سایبری به معنای:

- **استراتژی سایبری انطباق‌پذیر** : خودکارسازی در سرتاسر عملیات امنیتی، استراتژی سایبری انطباق‌پذیر و منعطفی را با تقویت توانایی تیم امنیتی برای مقیاس‌پذیری و سرعت فراهم می‌کند.
- **پاسخ‌های خودکار** : استفاده از قوانین خودکار برای پاسخ به شرایط مبتنی بر ویژگی‌های متعدد حوادث که پاسخ‌های خودکار را فعال می‌کنند و اقدامات متقابل را اجرا می‌کنند، در حالی که دفاع کنندگان را در فرآیند تصمیم‌گیری نگه می‌دارند.

جمع‌بندی

اصل "عملیات سایبری مؤثر" به سازمان‌ها امکان می‌دهد با سرعت به شرایط متغیر پاسخ دهند. این امر با دانستن نحوه تخصیص منابع در سطح، درک چگونگی رفع مؤثر حوادث در گذشته، و چگونگی رفتار احتمالی تهدیدات در حرکت به سمت رسیدن به اهداف شان آغاز می‌شود.

همان‌طور که سان تزو تأکید می‌کند: ***"سرعت، ماهیت جنگ است."*** در دفاع سایبری، توانایی عمل سریع، هوشمندانه و قاطع می‌تواند تفاوت بین یک نقض داده فاجعه‌بار و یک تلاش ناموفق برای نفوذ باشد. هدف نهایی ایجاد یک استراتژی دفاعی پویا و انطباق‌پذیر است که بتواند با چالش‌های دائماً در حال تغییر در فضای تهدید سازگار شود.

بخش سوم: حمله بدون درگیری (Attack without Conflict)

مقدمه

استراتژی به طور طبیعی از شناخت قابلیت‌های دفاعی خود، نقاط آسیب‌پذیر و چگونگی استفاده مهاجمان از این ضعف‌ها جریان می‌یابد. در عصر تهدیدات سایبری پیچیده، سازمان‌ها نیازمند استراتژی پیشگیرانه و منسجم هستند که ریشه در حکمت باستانی سان تزو دارد

اصول سان تزو در "حمله بدون درگیری"

سان تزو در فصل "حمله با استراتژی" از کتاب هنر جنگ، اصلی بنیادین را مطرح می‌کند: ***"بهترین پیروزی آن است که بدون جنگیدن به دست آید."*** او بر اهمیت شناخت قابلیت‌های نیروهای خود و نیروهای دشمن تأکید می‌کند.

سان تزو می‌گوید: ***"یک استراتژیست برتر دشمن را بدون جنگ شکست می‌دهد."*** این اصل در دفاع سایبری مدرن، به معنای پیش‌بینی و خنثی‌سازی تهدیدات قبل از آسیب‌رسانی آنهاست.

درک حملات پیچیده امروزی

- **طراحی دقیق حملات** : حملات پیچیده امروزی به دقت طراحی شده‌اند تا از آسیب‌پذیری‌ها در محیط‌های IT سازمانی بهره‌برداری کنند. هر مرحله از زنجیره حمله برای پیشبرد حمله به سمت هدف نهایی طراحی شده است.
- **اهداف متنوع مهاجمان** : اهداف مهاجمان متنوع است - از سرقت اعتبارنامه‌ها، تا نابودی داده‌های حیاتی، یا گروگان‌گیری داده‌های تجاری برای باج‌گیری.

مثال عملی: یک شرکت تولیدی با تجزیه و تحلیل الگوهای حمله در صنعت خود، توانست پیش‌بینی کند که کدام سیستم‌های کنترل صنعتی هدف احتمالی مهاجمان خواهند بود. با تقویت این سیستم‌ها و اجرای مانورهای دفاعی منظم، توانستند چندین تلاش نفوذ را قبل از آسیب‌رسانی خنثی کنند.

استراتژی هماهنگ و یکپارچه

سان تزو تأکید می‌کند: ***"مانند آب باشید که مسیر خود را با شرایط زمین تطبیق می‌دهد."*** این اصل در دفاع سایبری به معنای:

- **هماهنگی پاسخ‌ها** : تیم‌های امنیتی به استراتژی دفاعی هماهنگی نیاز دارند که شامل تکنیک‌ها و تاکتیک‌هایی است که از غافلگیری و فریب برای غلبه بر مهاجمان استفاده می‌کنند.
- **اتوماسیون و هماهنگی** : توانمندسازی محافظان برای هماهنگی بی‌درنگ و خودکارسازی اقدامات پاسخ در سراسر محیط از یک نقطه مرکزی، به آنها امکان می‌دهد بر محدودیت‌های مداخله دستی غلبه کنند.

هوشمندی تهدید و یکپارچه‌سازی

سان تزو می‌گوید: ***"شناخت دشمن و شناخت خود، در صد نبرد خطری متوجه شما نخواهد بود."*** در دفاع سایبری مدرن:

- **زمینه بلادرنگ** : یکپارچه‌سازی اطلاعات تهدید، زمینه حیاتی و بلادرنگی برای پیش‌بینی و کاهش تأثیر مخرب حملات فراهم می‌کند.
- **یکپارچه‌سازی جامع** : یکپارچه‌سازی با دامنه وسیعی از راهکارهای امنیتی - از جمله پلتفرم‌های SIEM، سیستم‌های حفاظت از نقاط پایانی و منابع اطلاعات تهدید - به سازمان‌ها امکان می‌دهد اقدامات پاسخ را در سراسر زنجیره امنیتی خود هماهنگ کنند.

خودکارسازی و انعطاف‌پذیری

سان تزو می‌گوید: ***"سرعت جوهره جنگ است."*** در دفاع سایبری مدرن:

- **خودکارسازی فراتر از پاسخ به حوادث** : قابلیت‌های هماهنگی از پاسخ به حوادث فراتر می‌روند و به سازمان‌ها امکان می‌دهند وظایف و جریان‌های کاری امنیتی روزمره را خودکار کنند.
- **انطباق‌با‌تاکتیک‌های در حال تکامل** : این اقدامات می‌توانند برای هدف قرار دادن تهدیدات خاص و انطباق با تاکتیک‌های در حال تکامل مهاجمان سایبری سفارشی‌سازی شوند.

تجزیه و تحلیل داده‌ها برای دفاع پیشگیرانه

سان تزو می‌گوید: ***"پیش‌بینی به معنای پیشگیری است."*** در دفاع سایبری:

- **هوشمندی در اقدام** : تجزیه و تحلیل داده‌ها به سازمان‌ها امکان می‌دهد استراتژی‌های دفاعی خود را در زمان واقعی با اطلاعات قابل اقدام تطبیق دهند.
- **یک گام جلوتر** : با تجزیه و تحلیل مداوم داده‌های تهدید و تنظیم اقدامات پاسخ بر اساس شرایط متغیر، سازمان‌ها می‌توانند یک گام جلوتر از مهاجمان خود باقی بمانند، تهدیدات را پیش‌بینی و خنثی کنند قبل از اینکه آسیبی وارد کنند.

جمع‌بندی

اصل "حمله بدون درگیری" نمایانگر تکامل دفاع سایبری از رویکرد واکنشی به رویکرد پیشگیرانه و استراتژیک است. در محیط تهدید سریع امروز، سازمان‌ها به پلتفرم امنیت سایبری نیاز دارند که بتواند با سرعت و پیچیدگی حملات مدرن همگام باشد.

با هماهنگی دقیق، خودکارسازی، و قابلیت‌های تحلیلی، سازمان‌ها می‌توانند دفاع سایبری خود را با دقت و چابکی تطبیق دهند، بهره‌گیری از اصول "حمله بدون درگیری" سان تزو برای غلبه بر تهدیدات قبل از وقوع آنها.

همان‌طور که سان تزو می‌گوید: ***"جنگ هنر فریب است."*** در دفاع سایبری، این به معنای ایجاد استراتژی‌هایی است که نه تنها از حملات جلوگیری می‌کنند، بلکه آنها را به سمت مسیرهای غلط هدایت می‌کنند، توانایی مهاجمان را برای شناسایی و بهره‌برداری از آسیب‌پذیری‌ها کاهش می‌دهند، و در نهایت، سازمان را بدون درگیری مستقیم با مهاجمان محافظت می‌کنند.

بخش چهارم: تأمین امنیت جبهه دیجیتال (Securing the Digital Front)

مقدمه

برنامه‌ریزی و آماده‌سازی می‌تولند نتیجه مثبت مقابله با یک حمله قریب‌الوقوع را از پیش تعیین کند. این اصل بنیادین در استراتژی دفاع سایبری ریشه در آموزه‌های سان تزو دارد.

اصول سان تزو در تأمین امنیت دیجیتال

سان تزو در فصل "آرایش‌های تاکتیکی" از کتاب هنر جنگ تأکید می‌کند: ***"نتیجه نبرد را می‌توان با آماده‌سازی و برنامه‌ریزی صحیح از پیش تعیین کرد."*** این اصل به همان اندازه در امنیت سایبری کاربرد دارد. یک استراتژی پیشگیرانه به محافظان امکان می‌دهد توانایی سازمان برای محافظت از دارایی‌های خود و حفظ عملیات را در هر شرایطی تضمین کنند.

مقابله با "استادان فرار"

سان تزو می‌گوید: ***"هنگامی که دشمن نقشه‌های شما را می‌داند، او می‌تواند از آنها فرار کند. اما وقتی نقشه‌های او را می‌دانید، می‌توانید او را محاصره کنید".***

- **تکنیک‌های پیچیده مهاجمان** : مهاجمان امروزی استادان فرار هستند که از تکنیک‌های پیچیده برای تضعیف راه‌حل‌های سنتی تشخیص استفاده می‌کنند تا جای پایی اولیه در یک دستگاه انتهایی، پلتفرمSaaS ، یا نقطه ورودی دیگر پیدا کنند، قبل از گسترش در شبکه به دنبال اهداف ارزشمندتر.
- **لزوم تسلط بر قابلیت مشاهده** : مقابله مؤثر با این "استادان فرار" مستلزم آن است که محافظان، استادان قابلیت مشاهده باشند و در صورت لزوم، از تکنیک‌های فریب استفاده کنند.

مثال عملی: یک شرکت مالی با استقرار سیستم‌های تله‌گذاری مانند هانی‌پات‌ها که اطلاعات جعلی را برای فریب مهاجمان ارائه می‌دادند، توانست چندین تلاش حمله را منحرف کند. مهاجمان زمان قابل توجهی را صرف تلاش برای استخراج "داده‌های حساس" از این سیستم‌های تله کردند، که به تیم امنیتی فرصت داد تا آنها را شناسایی و از شبکه اخراج کند.

دفاع با فریب

سان تزو می‌گوید: "جنگ مبتنی بر فریب است." این اصل در استراتژی دفاع سایبری به صورت زیر پیاده‌سازی می‌شود:

- **موقعیت‌یابی استراتژیک منابع** : دفاع با فریب مستلزم موقعیت‌یابی استراتژیک منابع و کنترل‌های امنیت سایبری برای محافظت از دارایی‌های حیاتی است.
- **لایه‌های دفاعی پیچیده** : بخش‌بندی شبکه و قراردادن مکانیسم‌های امنیتی برای ایجاد لایه‌های متعدد دفاعی که برای مهاجمان عبور از آنها دشوار است، به محافظان اجازه می‌دهد تا به سرعت اقدامات امنیتی و پروتکل‌های خود را برای مقابله با تاکتیک‌های مورد استفاده تهدیدات تنظیم کنند.

بینش و آگاهی از دارایی‌ها

سان تزو می‌گوید: ***"آنکه زمین و خود و دشمن را می‌شناسد، پیروز خواهد شد."*** در امنیت سایبری:

- **مشـاهده متمرکز دارایی‌ها** : قابلیت مشـاهده متمرکز دارایی‌ها، از جمله دسـتگاه‌ها و اشـیاء کاربری، و همچنین ارتباط بین این اشـیاء در یکپارچه‌سـازی‌های مختلف، به محافظان امکان می‌دهد برای هر دارایی، نوع دارایی یا گروه دارایی برچسب ایجاد کنند.

- **ارزش‌گذاری خودکار** : این امکان را برای محافظان فراهم می‌کند تا به طور خودکار ارزش مناسـب دارایی را بر اسـاس ریسـک اعمال کنند. این زمینه در قالبی ارائه می‌شـود که به آنها امکان می‌دهد وضـعیت فعلی را در هنگام بررسی ارزیابی کنند.

یکپارچه‌سازی و مدیریت

سـان تزو بر اهمیت هماهنگی و یکپارچگی تأکید می‌کند: ***"فرماندهی پنج عنصـر در جهت‌های مختلف منجر به پیروزی می‌شود."*** در دفاع سایبری مدرن:

- **حداقل پیکربندی** : یکپارچه‌سـازی‌ها برای به حداقل رسـاندن مدیریت پیکربندی و ارائه قابلیت مشـاهده کامل و زمینه‌ای به دارایی‌ها طراحی شده‌اند.

- **بررسـی صـحت** : علاوه بر این، بررسـی‌های صـحت و سـلامت سـامانه‌ها برای اطمینان از عملکرد صـحیح یکپارچه‌سازی‌ها و آسیب‌پذیر نبودن دارایی‌ها در برابر حمله فراهم می‌شود.

مدیریت متمرکز نقاط پایانی

سان تزو می‌گوید: ***"ارتش متحد قدرتمندتر است."*** در امنیت نقاط پایانی:

- **مدیریت متمرکز رایانه‌ها و لپ‌تاپ‌ها** : متمرکزسـازی پیکربندی‌های نظارت و محافظت از تجهیزات رایلنه‌ای در یک پلتفرم واحد، استقرار و پیکربندی ماژول‌های متعدد را ساده می‌کند.

- **بینش یکپارچه** : قرار دادن این پیکربندی‌های کلاینت در یک مکان، بینش و زمینه یکپارچه‌ای را در عملیات امنیت سایبری فراهم می‌کند، در حالی که اثربخشی آنها را به حداکثر می‌رساند.

جمع‌بندی

آماده‌سـازی و برنامه‌ریزی اجزای حیاتی هر اسـتراتژی امنیت سـایبری هسـتند که به محافظان قابلیت مشـاهده، زمینه و کنترل‌های مورد نیاز برای جلوگیری از تبدیل تهدیدات به حملات را می‌دهند. اطلاعات تهدید یکپارچه در یک مکان واحد، به محافظان امکان می‌دهد برای هر تکنیک سـایبری فریبکارانه و سـازگارپذیر که با آن مواجه می‌شـوند آماده باشـند – در نهایت نتیجه مثبت برای حملات آینده را از پیش تعیین می‌کنند.

همان‌طور که سـان تزو می‌گوید: ***"پیروزی قبل از نبرد تضـمین می‌شـود."*** در دفاع سـایبری، این به معنای ایجاد استراتژی‌هایی است که نه تنها در زمان وقوع حمله واکنش نشان می‌دهند، بلکه محیطی ایجاد می‌کنند که در آن:

۱. تهدیدها به سرعت شناسایی می‌شوند

۲. دارایی‌های حیاتی به خوبی محافظت می‌شوند

۳. مهاجمان در لایه‌های دفاعی پیچیده گمراه می‌شوند

۴. و ابزارهای لازم برای عمل سریع و قاطع در دسترس هستند

با این آماده‌سازی دقیق، سازمان‌ها می‌توانند نه تنها به حملات پاسخ دهند، بلکه می‌توانند از پیروزی در "نبرد" آینده سایبری اطمینان حاصل کنند، حتی قبل از شروع آن.

بخش پنجم: بهینه‌سازی تاب‌آوری سایبری (Optimizing Cyber Resilience)

مقدمه

محافظ هوشمند، دفاعی یکپارچه و هماهنگ را با استفاده از انرژی ترکیبی تمامی منابع موجود برای مقابله با تهدیدات پیچیده و ترکیبی امروزی برپا می‌کند. این استراتژی ریشه در آموزه‌های سان تزو دارد و به یک رویکرد منسجم و جامع برای دفاع سایبری منتهی می‌شود.

اصول سان تزو در بهینه‌سازی تاب‌آوری

سان تزو در فصل "انرژی" از کتاب هنر جنگ، رهبران را تشویق می‌کند تا قدرت را از طریق توان جمعی نیروهای ترکیبی ایجاد کنند، به جای اینکه به افراد برای پیشبرد امور تکیه کنند. او می‌گوید: ***"انرژی در جنگ، مانند کمان کشیده‌ای است که به سرعت رها می‌شود".***

این استراتژی در امنیت سایبری با اجرای رویکردی جامع و کل‌نگر که تلاش‌ها را در سراسر افراد، فرآیندها و فناوری هماهنگ می‌کند، قابل اجراست تا موضع دفاعی متحد و قدرتمندی در برابر تهدیدات سایبری امروزی تضمین شود.

چالش صنعت امنیت سایبری واکنشی

سان تزو می‌گوید: ***"در جنگ، کار ما ابتدا شکست‌ناپذیر کردن خودمان و سپس منتظر آسیب‌پذیری دشمن ماندن است".***

- **تاریخچه واکنشی** : برای دهه‌ها، صنعت امنیت سایبری واکنشی بوده است. با هر تهدید امنیتی جدید، یک فروشنده امنیتی یا استارتاپ راهی برای مقابله پیدا می‌کرد، ابزاری توسعه می‌داد و آن را به مشتریان عرضه می‌کرد.
- **چالش یکپارچه‌سازی** : با تکامل و پیچیده‌تر شدن تهدیدات، تیم‌های امنیتی با وظیفه یکپارچه‌سازی ده‌ها ابزار که برای کار در یک سیلو طراحی شده بودند، مواجه شدند. طبق گزارش Panaseer 2022 ، سازمان‌ها به طور متوسط از ۷۶ ابزار در محیط امنیتی خود استفاده می‌کنند.
- **اشباع هشدار** : محافظان از هشدارهای این ابزارهای منفرد اشباع شده‌اند، که مرتبط‌سازی و اولویت‌بندی برای ایجاد دفاع هماهنگ از دارایی‌های حیاتی سازمان را دشوار می‌سازد.

مثال عملی: یک شرکت خدمات مالی با بیش از ۶۰ ابزار امنیتی مجزا مواجه بود که هزاران هشدار روزانه تولید می‌کردند. با پیاده‌سازی یک پلتفرم یکپارچه با قابلیت‌های تحلیلی پیشرفته، آنها توانستند هشدارها را بیش از ۸۵٪ کاهش دهند، به تیم امنیتی اجازه دهند بر تهدیدات واقعی تمرکز کنند و زمان پاسخ به حوادث را از روزها به ساعت‌ها کاهش دهند.

نوآوری مداوم برای مقابله با تهدیدات

سان تزو می‌گوید: ***"همانطور که آب شکل خود را به شرایط زمین وفق می‌دهد، در جنگ نیز باید خود را با دشمن تطبیق دهیم".***

- **سازگاری مداوم** : محافظان باید از رقبا پیشی بگیرند و به طور مداوم استراتژی و قابلیت‌های دفاع سایبری خود را در پاسخ به تهدیدات و تاکتیک‌های در حال تکامل نوآوری کرده و تطبیق دهند.

- **مکانیسم‌های دفاعی متنوع ولی‌نه موازی** : این شامل اصلاح مکانیسم‌های دفاعی برای مقابله با آسیب‌پذیری‌های جدید، بازیگران تهدید، دفاع مستقیم (فایروال‌ها، آنتی‌ویروس، امنیت نقطه پایانی و غیره) و فناوری فریب سایبری غیرمستقیم (هانی‌پات‌ها، تله‌ها) است.

تشدید کننده‌های نیرو برای دفاع یکپارچه

سان تزو می‌گوید: ***"پس از فهم فواید پنج عنصر، من با کمک نیروهای کمکی موفقیت را به دست می‌آورم".***

- **عمل به عنوان تشدید کننده‌های نیرو** : برای پیشی گرفتن از رقبا، محافظان باید به عنوان تشدید کننده‌های نیرو عمل کنند و تشخیص و مهندسی پاسخ خود را در یک دفاع متحد و یکپارچه ترکیب کنند.
- **بهینه‌سازی منابع موجود** : *پرتاب پول به سمت مشکل راه‌حل نیست.* راه‌حل بهتر، یکپارچه‌سازی همه ابزارهای امنیتی موجود است که یک راه‌حل امنیت سایبری کارآمد را برای محافظان فراهم می‌کند، عملیات را ساده می‌کند، بهره‌وری محافظان را افزایش می‌دهد و در سطح وسیع مقیاس‌پذیر است.

کتابچه‌های راهنمای استراتژیک

سان تزو می‌گوید: ***"فرمانده ماهر برنامه‌ای دقیق برای قبل، حین و پس از نبرد دارد".***

- **اقدامات منسجم و از پیش تعیین شده** : کتابچه‌های راهنما (cook books) به محافظان راهنمای استراتژیک با دستورالعمل‌های گام به گام برای انجام وظایف معمول ارائه می‌دهند. استفاده از این کتاب‌های راهنمای خودکار اطمینان می‌دهد که رویه‌های امنیتی به شیوه‌ای قابل اعتماد، سازگار و کارآمد انجام می‌شوند.
- **پاسخ هماهنگ** : این پیکربندی اجازه پاسخ هماهنگ به هر وضعیتی را قبل از وقوع آن می‌دهد و امکان اجرای مناسب دستورالعمل‌های گام به گام را با هماهنگی با سایر کنترل‌ها فراهم می‌کند.

بازیابی و تاب‌آوری

سان تزو می‌گوید: ***"فرمانده برتر به هنگام شکست فرصت‌های بازیابی را می‌شناسد".***

- **اقدامات مستقیم و غیرمستقیم** : یکپارچه‌سازی بازیابی با قابلیت‌های دفاعی، ترکیبی تاکتیکی از اقدامات مستقیم و غیرمستقیم را به محافظان ارائه می‌دهد که از دارایی‌های دیجیتال در برابر حمله باج‌افزار محافظت می‌کند، تأثیر حمله را کاهش می‌دهد و اجازه می‌دهد سیستم‌ها به سرعت و به شکلی غیرتخریبی بازیابی شوند.
- **آمادگی قبلی** : با ایجاد نسخه‌های پشتیبان منظم از زیرساخت‌های حیاتی در اولین نشانه حمله، زمان بازیابی آخرین نسخه سالم تسریع می‌شود.

جمع‌بندی: استراتژی دفاعی یکپارچه

تهدیدات امروزی چندوجهی، بسیار گریزان و فزاینده پیچیده هستند. برای پیشی گرفتن از رقبا، محافظان باید به عنوان تشدید کننده‌های نیرو عمل کنند و تشخیص و مهندسی پاسخ خود را در دفاعی یکپارچه و متحد ترکیب کنند که بین تیم‌ها، ابزارها و فرآیندهای ناهمگون هماهنگی ایجاد می‌کند تا تهدیدات را شناسایی، تأثیر آنها را کاهش و سیستم‌ها را به سرعت و بدون اختلال بازیابی کند.

این استراتژی هیبریدی مستلزم نوآوری و یکپارچه‌سازی مداوم در سراسر یک زنجیره امنیتی همواره در حال گسترش است که قابلیت مشاهده و کنترل مورد نیاز محافظان را در سرتاسر محیط تهدید برای محافظت از سازمان به شیوه‌ای مؤثرتر، کارآمدتر و سازگارتر فراهم می‌کند.

همان‌طور که سان تزو می‌گوید: "هماهنگی نیروها، نه تعداد آنها، پیروزی را تضمین می‌کند." در دفاع سایبری مدرن، این به معنای ایجاد یک استراتژی تاب‌آوری سایبری بهینه‌شده است که:

۱. منابع دفاعی را هماهنگ می‌کند
۲. عملیات را ساده می‌سازد
۳. پاسخ‌های از پیش تعیین‌شده را خودکار می‌کند
۴. بازیابی سریع را تضمین می‌کند
۵. و یک موضع دفاعی یکپارچه ایجاد می‌کند که بزرگتر از مجموع اجزای آن است

با این رویکرد استراتژیک و یکپارچه، سازمان‌ها می‌توانند حتی در مواجهه با پیچیده‌ترین تهدیدات سایبری، انعطاف‌پذیری و استحکام خود را حفظ کنند.

بخش ششم: مدیریت آسیب‌پذیری و دارایی (Vulnerability and Asset Management)

مقدمه

شناسایی و تقویت نقاط ضعف در محیط خود برای مختل کردن اهداف مهاجمان یک استراتژی کلیدی در دفاع سایبری است. این رویکرد ریشه در آموزه‌های سان تزو دارد و اهمیت شناخت آسیب‌پذیری‌های خود و استفاده از نقاط ضعف دشمن را برجسته می‌کند.

اصول سان تزو در مدیریت آسیب‌پذیری و دارایی

سان تزو در فصل "نقاط ضعف و قوت" از کتاب هنر جنگ، جنگجویان را تشویق می‌کند تا تلاشی برای شناسایی نقاط ضعف هم در ارتش خود و هم در ارتش دشمنان‌شان صرف کنند. او می‌گوید: ***"شناخت خود و دشمن، ضامن پیروزی در صد نبرد است".***

این بینش‌ها برای تقویت دفاع و یافتن راه‌هایی برای بهره‌برداری از ضعف‌های دشمنان استفاده می‌شود. این استراتژی در امنیت سایبری نیز کاربرد دارد: دانستن نقاط آسیب‌پذیر خود و مهاجمان برای تقویت دفاع از دارایی‌های حیاتی در معرض خطر و بهره‌برداری از ضعف‌های مهاجمان بالقوه ضروری است.

درک محیط تهدید دوطرفه

سان تزو می‌گوید: ***"حمله جایی صورت می‌گیرد که دفاع وجود ندارد."*** در دنیای سایبری:

- **آسیب‌پذیری‌های همه‌جا حاضر** : تهدیدات سایبری امروزی دائماً اینترنت و سایر شبکه‌ها را برای آسیب‌پذیری‌هایی که می‌توانند از آنها بهره‌برداری شود، جستجو می‌کنند. پیکربندی‌های نادرست، APIهای متن‌باز، فایلهای فراموش شده ابری و برنامه‌های غیرمجاز تقریباً در هر جایی که یک مهاجم کنجکاو تصمیم به جستجو بگیرد، یافت می‌شوند.
- **آسیب‌پذیری دو طرفه** : خوشبختانه، این خیابان دو طرفه است. بازیگران تهدید نیز نسبت به همان آسیب‌پذیری‌هایی که زیرساخت‌های سازمانی را تهدید می‌کنند، آسیب‌پذیر هستند و مستعد اقدامات متقابل دفاعی هستند که می‌تواند قابلیت‌های حمله آنها را مختل کند یا از بین ببرد.

مثال عملی: یک شرکت فناوری با شناسایی پروتکل‌های ارتباطی مورد استفاده توسط یک باج‌افزار خاص، توانست قوانین فایروال خود را برای مسدود کردن این پروتکل‌ها پیکربندی کند. این اقدام پیشگیرانه نه تنها شرکت را در برابر باج‌افزار محافظت کرد، بلکه از گسترش آن در شبکه‌های همکار نیز جلوگیری نمود.

شناسایی و ارزیابی مداوم

سان تزو می‌گوید: ***"کسی که دشمن را می‌شناسد و خود را می‌شناسد، در صد نبرد شکست نخواهد خورد."*** در امنیت سایبری:

- **ارزیابی مستمر** : محافظان باید به طور مداوم نقاط قوت و ضعف امنیت سایبری سازمان خود و همچنین نقاط قوت و ضعف مهاجمان سایبری بالقوه را شناسایی و ارزیابی کنند.

- **شناسایی دارایی‌های حیاتی** : ابتدا لازم است دارایی‌های بحرانی در سازمان شناسایی شوند و ارزش دارایی اولویت‌بندی شود، سپس حفاظت‌ها در اطراف آنها تقویت گردد.
- **جستجوی شکاف‌ها** : همزمان، محافظان باید به دنبال شکاف‌های موجود در قابلیت‌های مهاجمان باشند و از اطلاعات تهدید پیشرفته برای شناسایی و بهره‌برداری از نقاط ضعف در تاکتیک‌ها و بدافزارهای آنها استفاده کنند.

اولویت‌بندی بر اساس ارزش و ریسک

سان تزو می‌گوید: ***"جنگجوی برتر قبل از نبرد، نقطه تصمیم‌گیری را می‌جوید و در آنجا تمرکز می‌کند."*** در دفاع سایبری:

- **درک عمیق محیط دیجیتال** : این امر مستلزم درک عمیق محیط دیجیتال - از جمله معماری شبکه، جریان‌های داده و دارایی‌های حیاتی - است تا بتوان به طور استراتژیک دفاع را در مکان‌هایی قرار داد که گلوگاه‌های طبیعی را اهرم می‌کنند و آسیب‌پذیری‌ها را کاهش می‌دهند یا برطرف می‌کنند.
- **تنظیم پویای ارزش دارایی** : قوانین دارایی به محافظان امکان می‌دهد تا ارزش یک دارایی را بر اساس اولویت‌بندی حوادث و چارچوب MITRE ATT&CK به صورت پویا تنظیم کنند. استفاده از قوانین و فیلترهای شرطی برای تعیین ارزش دارایی برای کسب‌وکار، به شما امکان می‌دهد طبقه‌بندی داده‌ها، آسیب‌پذیری‌ها و بازیابی را اولویت‌بندی کنید.

هوشمندی و تشخیص تهدید

سان تزو می‌گوید: ***"دانش پیشین نمی‌تواند از کتاب‌ها به دست آید یا از محاسبات ناشی شود. آن را باید از افرادی کسب کرد که با دشمن آشنا هستند."*** در امنیت سایبری:

- **تمایز بین هشدارها و حوادث** : تشخیص تفاوت بین هشدارها و حوادث برای محافظان مهم است. یک هشدار فقط نشانه‌ای است که چیزی غیرعادی رخ داده است. یک حادثه، تأییدی است بر یک حمله واقعی.
- **تأیید تهدید** : هوشمندی تهدید به محافظان امکان می‌دهد موارد قابل مشاهده - مانند هش‌ها، آدرس‌های IP و URLهای مخرب شناخته شده - را برای تأیید وجود احتمالی حملات قرار دهند.

خودکارسازی و بصیرت در مورد مهاجمان

سان تزو می‌گوید: ***"سریع باش مانند باد، آرام مانند جنگل، مهاجم مانند آتش، بی‌حرکت مانند کوه."*** در دفاع سایبری:

- **هوشمندی خودکار** : فیدهای هوشمندی تهدید به محافظان امکان می‌دهد از جریان‌های کاری خودکارسازی برای ایجاد پویای لیست‌های انسداد قوی برای دامنه‌ها، آدرس‌های IP و هش‌ها یا هر محتوای قابل قبول برای یک دستگاه قابل پیکربندی استفاده کنند.
- **درک قابلیت‌های مهاجمان** : این به محافظان بینشی در مورد قابلیت‌ها و ضعف‌های مهاجمان می‌دهد، به طوری که می‌توانند اقدامات متقابل مؤثری را برای مختل کردن و خلع سلاح بازیگران تهدید بالقوه به کار گیرند.

- **گسترش هوشمندی داخلی** : محافظان می‌توانند هوشمندی داخلی خود را به قطع ارتباط خارجی و محدود کردن حرکت به مهاجمان خود به عنوان عاملی تخفیف‌دهنده برای ضعف‌های موجود در محیط محافظ گسترش دهند.

مدیریت یکپارچه آسیب‌پذیری

سان تزو می‌گوید: ***"آماده‌سازی دفاع نشان‌دهنده قدرت واقعی است."*** در امنیت سایبری:

- **مدیریت جامع آسیب‌پذیری** : مدیریت آسیب‌پذیری می‌تواند با مدیریت دارایی ترکیب شود تا بینش‌های لازم برای تقویت دفاع خود را در اختیار محافظان قرار دهد و همزمان به نقاط ضعف مهاجمان حمله کند.
- **قابلیت مشاهده و اولویت‌بندی** : این امکان را فراهم می‌کند تا با ارائه قابلیت مشاهده به دارایی‌های دیجیتال، توانایی اولویت‌بندی آنها بر اساس ارزش و آسیب‌پذیری، و ریسک نقض، محافظان بتوانند آسیب‌پذیری‌ها را بر اساس آن اولویت‌بندی به سرعت برطرف کنند.

جمع‌بندی

مدیریت آسیب‌پذیری و دارایی یک استراتژی کلیدی دفاع سایبری است که بر شناسایی، اولویت‌بندی و تقویت نقاط ضعف در محیط خودی متمرکز است، در حالی که همزمان از نقاط ضعف مهاجمان برای مختل کردن حملات آنها استفاده می‌کند.

با درک عمیق از محیط دیجیتال، تخصیص ارزش به دارایی‌ها، و استفاده از هوشمندی تهدید، محافظان می‌توانند یک استراتژی دفاعی چندلایه ایجاد کنند که هم از دارایی‌های حیاتی محافظت می‌کند و هم قابلیت‌های مهاجمان را مختل می‌سازد.

همان‌طور که سان تزو می‌گوید: ***"نبرد را قبل از آغاز آن ببرید."*** در دفاع سایبری، این به معنای:

۱. شناسایی و تقویت نقاط ضعف خود قبل از اینکه مهاجمان بتوانند از آنها بهره‌برداری کنند

۲. درک و بهره‌برداری از نقاط ضعف مهاجمان برای خنثی کردن حملات آنها

۳. ایجاد یک رویکرد پیشگیرانه که از حمله جلوگیری می‌کند، نه فقط پاسخ به آن

۴. اولویت‌بندی منابع محدود برای محافظت از آنچه بیشترین اهمیت را دارد

با این استراتژی متوازن، سازمان‌ها می‌توانند نه تنها از خود محافظت کنند، بلکه یک مانع بازدارنده قدرتمند برای حملات آینده ایجاد کنند.

بخش هفتم: تاکتیک‌های سایبری انطباق‌پذیر (Adaptive Cyber Tactics)

مقدمه

برتری بر مهاجمان نیازمند انعطاف‌پذیری و کنترل دقیق بر زنجیره امنیتی اســـت تا مؤثرترین اقدامات متقابل به کار گرفته شوند. این اصل از فصل "مانور" در کتاب هنر جنگ سان تزو الهام گرفته است.

اصول سان تزو در تاکتیک‌های سایبری انطباق‌پذیر

سان تزو در فصل ۷ کتاب هنر جنگ، "مانور"، بر اهمیت استقرار نیروها به گونه‌ای تأکید می‌کند که نقاط قوت شما را در برابر نقاط ضعف دشمن قرار دهد. او می‌گوید: ***"در جنگ، مانور بهترین سیاست است".***

این اصـل در امنیت سـایبری با اطمینان از انعطاف‌پذیری و کنترل دقیق بر زنجیره امنیتی برای اسـتقرار مناسـب‌ترین ابزارها و تکنیک‌ها در طول چرخه عمر یک حمله - قبل، حین و بعد از آن - کاربرد دارد.

سنجش قابلیت‌های پیشگیری و تشخیص

ســـان تزو می‌گوید: ***"کســـی که قبل از جنگ محاســـبات زیادی در معبد انجام می‌دهد، پیروز می‌شـــود."*** در امنیت سایبری:

- **اولویت پیشـگیری** : در امنیت سـایبری، اولویت با پیشـگیری اسـت - پیشـگیری باید قوی‌تر از توانایی تشـخیص و پاسـخ باشـد. این مدل به محافظان امکان می‌دهد درک دقیقی از ترکیب تهدید در ویژگی‌ها، رفتارها، مشـخصـات و اقدامات مؤثر برای خنثی کردن آن در طول کل خط زمانی حادثه داشته باشند.
- **بازی موش و گربه** : دفاع سایبری مدت‌هاست که به *بازی موش و گربه* تبدیل شده است. هر بار که تهدید جدیدی ظاهر می‌شود، صنعت برای توسعه ابزار جدیدی عجله می‌کند که معمولاً در سراسر زنجیره امنیتی سازمان یکپارچه نیست.

مثال عملی: یک سازمان مراقبت‌های بهداشتی با وجود ده‌ها ابزار امنیتی جداگانه، هنوز با تأخیر در تشخیص و پاسخ به حملات مواجه بود. با پیاده‌ســـازی یک پلتفرم متمرکز که این ابزارها را یکپارچه می‌کرد، آنها توانســـتند زمان تشـــخیص را از روزها به دقایق کاهش دهند و پاسخ‌های خودکار را برای جلوگیری از حملات مشابه در آینده فعال کنند.

چالش یکپارچه‌سازی و نیاز به کنترل متمرکز

سان تزو می‌گوید: ***"فرماندهی لشکر مانند فرماندهی یک نفر است، مسئله، سازماندهی است."*** در امنیت سایبری:

- **ابزارهای متعدد بدون یکپارچگی** : در نتیجه، اکثر سازمان‌ها ده‌ها ابزار امنیتی را مستقر می‌کنند که به شناسایی، پیشگیری و حل علائم امنیتی کمک می‌کنند، اما برای رفع مشکلات سیستمی در سازمان یکپارچه نیستند.
- **نقطه کنترل یکپارچه** : محافظان امروزی به نقطه کنترلی نیاز دارند که قبل، حین و بعد از حمله، با یکپارچه‌سازی بی‌درنگ طیف وسیعی از ابزارهای امنیت سایبری از طریق رویکردی باز بدون محدودیت فروشنده عمل کند.

آگاهی موقعیتی و هوشمندی تطبیقی

سان تزو می‌گوید: ***"آب شکل ظرف خود را به خود می‌گیرد، جنگ شکل دشمن خود را."*** در امنیت سایبری:

- **آگاهی از سطح حمله** : این امر آگاهی موقعیتی از سطح حمله گسترش‌یابنده و درک زمینه‌ای ایجاد می‌کند - با فراهم کردن قابلیت مشاهده دارایی‌های دیجیتال و هرگونه نقاط ضعف یا آسیب‌پذیری‌هایی که می‌توانند به صورت پیشگیرانه برطرف شوند.
- **قابلیت‌های تطبیقی** : این قابلیت‌های تطبیقی همچنین در حین حمله گسترش می‌یابند و به محافظان آگاهی موقعیتی بلادرنگ از حمله در حال پیشرفت را می‌دهند، به دنبال آن توصیه‌های اقداماتی برای کاهش سریع ارائه می‌شود.
- **یادگیری مستمر** : سپس، پس از یک حمله، سیستم داده‌های مرتبط را جمع‌آوری می‌کند تا توصیه‌های با پشتیبانی هوش مصنوعی را برای جلوگیری از حملات مشابه در آینده ارائه دهد، در حالی که عملیات‌های تجاری را ادامه می‌دهد.

خودکارسازی و واکنش سریع

سان تزو می‌گوید: ***"سرعت، جوهره جنگ است."*** در امنیت سایبری:

- **قوانین و محرک‌های خودکارسازی** : این امر توانایی محافظان برای کار با مقیاس و سرعت ماشین را افزایش می‌دهد تا تأثیر حملات را شناسایی، کاهش یا متوقف کنند. حوادث شناسایی شده می‌توانند پاسخ‌های خودکار و اقدامات متقابل از پیش تأیید شده را فعال کنند.
- **اقدامات از پیش تأیید شده** : اقدامات مانند گرفتن مستمر نسخه‌های پشتیبان یا قرنطینه بلادرنگ سیستم آلوده. این کار زمان پاسخ را تسریع می‌کند و واکنش‌ها را در سراسر سازمان مؤثرتر می‌سازد.

منوی محوری حوادث برای اقدام سریع

سان تزو می‌گوید: ***"تصمیمات فرمانده باید مانند سرعت برق باشد."*** در امنیت سایبری:

- **اقدام سریع در زنجیره حمله** : منوهای از پیش ایجاد شده تجهیزات امنیتی در هنگام بروز حوادث به محافظان امکان می‌دهند با ارائه مجموعه‌ای از پیش تأیید شده از اقداماتی که می‌توانند برای توقف حملات و کاهش تأثیر آنها انجام دهند، به سرعت در هنگام گسترش زنجیره حمله عمل کنند.
- **مدیریت پیشاپیش** : اقدامات از قبل تنظیم، مدیریت و تأیید می‌شوند توسط محافظانی که سپس می‌توانند این **"تیرها در ترکش"** را به سرعت و مؤثر، هنگامی که بیشترین اهمیت را دارد، مستقر کنند.

رویدادهای هوشمندی تهدید و تحلیل زنجیره حمله

سان تزو می‌گوید: ***"شناخت دشمن و شناخت خود، در صد نبرد خطری متوجه تو نخواهد بود."*** در امنیت سایبری:

- **دریافت منابع متعدد هوشمندی** : سیستم چندین فید اطلاعات تهدید را از منابع متعدد دریافت می‌کند و سپس این اطلاعات را به وضعیت منحصر به فرد سازمان و محیط IT آن اعمال می‌کند.

- **شناسایی حمله جاری** : این امر به شناسایی حمله در حال انجام، تعیین تکنیک‌هایی که استفاده می‌کند و اقدام احتمالی بعدی آن کمک می‌کند - همه با هدف کمک به محافظان برای انتقال از جریان‌های کاری واکنشی به پیشگیرانه.
- **تحلیل پس از واقعه** : رویدادهای هوشمندی تهدید به محافظان کمک می‌کند زنجیره حمله را پس از وقوع تحلیل کنند و توصیه‌هایی برای پر کردن شکاف امنیتی و بهبود جریان‌های کاری واکنشی ارائه دهند.

نیاز به کنترل مرکزی برای محیط‌های پیچیده

سان تزو می‌گوید: ***"کنترل جمعیت زیاد مانند کنترل تعداد کمی است، مسئله سازماندهی است."*** در امنیت سایبری مدرن:

- **محیط‌های پیچیده** : با ادامه گسترش و پیچیده‌تر شدن زنجیره امنیتی، محافظان به یک نقطه کنترل مرکزی نیاز دارند که از آن بتوانند مانور مناسب را در برابر تهدیدات نوظهور مستقر کنند.
- **مرکز فرماندهی یکپارچه** : این مرکز فرماندهی مرکزی، آگاهی موقعیتی از وضعیت امنیت سایبری در محیط‌های IT، توانایی هماهنگی پاسخ‌های حادثه به سرعت و بازگرداندن سیستم‌های آسیب‌دیده به حالت عملیاتی عادی، و بینش برای بستن شکاف‌های امنیتی به روشی غیرمخرب را فراهم می‌کند.

جمع‌بندی

تاکتیک‌های سایبری انطباق‌پذیر، به سازمان‌ها انعطاف‌پذیری را می‌دهد تا ابزارها و تکنیک‌های مناسب را در سراسر چرخه عمر یک حمله مستقر کنند. این رویکرد یکپارچه به محافظان امکان می‌دهد:

۱. تهدیدات را پیش از آنکه حملات تبدیل شوند، شناسایی و پیشگیری کنند

۲. به حملات در جریان با سرعت و دقت پاسخ دهند

۳. از حوادث برای تقویت دفاع آینده بیاموزند

۴. از یک نقطه کنترل مرکزی به منظور هماهنگ‌سازی تمام فعالیت‌های دفاعی استفاده کنند

همان‌طور که سان تزو می‌گوید: ***"در هرج و مرج، فرصت نهفته است."*** در امنیت سایبری، سازمان‌هایی که می‌توانند تاکتیک‌های انطباق‌پذیر را به کار گیرند، می‌توانند آشفتگی یک حمله را به فرصتی برای تقویت دفاع خود تبدیل کنند. آنها با داشتن ابزارهای درست، یکپارچه شده در یک پلتفرم منسجم، قادر خواهند بود تهدیدات را در سراسر کل زنجیره حمله متوقف کنند و انعطاف‌پذیری امنیتی خود را به طور مداوم افزایش دهند.

هشتم: استراتژی‌های متنوع امنیت سایبری (Diversified Cybersecurity Strategies)

مقدمه

اســـتفاده از مجموعه کامل اســـتراتژی‌ها و تاکتیک‌های امنیت ســـایبری در دســـترس، راهی کارآمد و مؤثر برای حفظ تعادل مهاجمان است. این رویکرد ریشه در فصل هشتم کتاب هنر جنگ سان تزو دارد و بر اهمیت تنوع در تاکتیک‌های دفاعی تأکید می‌کند.

اصول سان تزو در استراتژی‌های متنوع امنیت سایبری

ســـان تزو در فصـــل هشـــتم کتاب هنر جنگ، "تنوع در تاکتیک‌ها"، به جنگجویان یادآوری می‌کند که از مجموعه کامل اســتراتژی‌ها و تکنیک‌هایی که در هفت فصـل اول آموخته‌اند، به بهترین شـکل اسـتفاده کنند. او می‌گوید: ***"نظامی که مبتکر نیست، هرگز غافلگیر نمی‌کند و هرگز پیروز نمی‌شود".***

این زمان مناسـبی در "هنر دفاع" اسـت تا درنگ کرده و بررسـی کنیم چگونه بهترین اسـتفاده را از اسـتراتژی‌ها و تاکتیک‌های امنیت سایبری که آموخته‌ایم، در عمل به کار ببندیم.

چالش منابع و تخصص نامتوازن

ســـان تزو می‌گوید: ***"فرمانده باید بداند چگونه پنج مزیت را به کار ببندد: وقتی می‌داند چه زمانی و مکانی برای نبرد مناسب است، ارتش او پیروز خواهد شد".***

- **عدم توازن منابع** : برخی تیم‌های امنیتی از تخصـــص فراوان برخوردارند اما ابزار یا زمان کافی برای اجرای یک اسـتراتژی موفق ندارند. برخی دیگر مجموعه ابزار عمیق دارند اما تخصـص یا زمان لازم برای بهینه‌سـازی اسـتفاده از آنها را ندارند. برخی تمام وقت دنیا را دارند اما تخصص یا منابع اندکی دارند.
- **چالش جامعیت** : تعداد بسیار کمی از تیم‌های امنیتی هر سه عامل را دارند (افراد، فرآیند، فناوری)، که اجرای حتی محکم‌ترین اسـتراتژی‌های امنیت سـایبری را دشـوار می‌سـازد. این ناهماهنگی، به کارگیری تاکتیک‌های مناسـب در زمان مناسب را دشوار می‌کند و منجر به افزایش خطر یک نقض تأثیرگذار می‌شود.

مثال عملی: یک شرکت متوسط با تنها دو متخصص امنیت سایبری، علی‌رغم سرمایه‌گذاری در ابزارهای متعدد، با حمله موفق باج‌افزار مواجه شد. بررسی پس از حادثه نشان داد که تیم امنیتی آنها نه زمان کافی برای پیکربندی مناسب ابزارها را داشت و نه دانش لازم برای تفســـیر هشـــدارهای تولید شـــده را. با پیاده‌ســـازی یک پلتفرم یکپارچه که راهنمایی‌های آماده و دستورالعمل‌های گام به گام را ارائه می‌داد، آنها توانستند تأثیرگذاری تیم کوچک خود را به طور قابل توجهی افزایش دهند.

پر کردن شکاف‌ها با راهنمایی متمرکز

سان تزو می‌گوید: ***"آن کس که دشمن را خوب می‌شناسد و خود را خوب می‌شناسد، در صد نبرد پیروز خواهد شد."*** در امنیت سایبری مدرن:

- **نقطه کنترل مرکزی** : محافظان به یک نقطه کنترل مرکزی نیاز دارند که از آن بتوانند طیفی از اســـتراتژی‌های امنیت سـایبری را مسـتقر کنند، تهدیدات را به چالش بکشـند و اسـتراتژی‌های دفاعی را با پیشـرفت تهدیدها تطبیق دهند.

- **پر کردن شـکاف‌ها** : این رویکرد این شـکاف‌ها را پر می‌کند و به تیم‌ها راهنمایی، منابع و کارایی عملیاتی لازم را می‌دهد تا استراتژی‌ها و تکنیک‌های در دسترس خود را در عمل پیاده کنند.

عمل در سراسر چرخه حیات حمله

سـان تزو می‌گوید: ***"جنگجوی برتر ابتدا خود را شـکسـت‌ناپذیر می‌سـازد، سـپس فرصـت شـکسـت دادن دشـمن را می‌جوید."*** در امنیت سایبری:

- **رویکرد فراگیر** : کار در سـراسـر چرخه حیات حمله، به محافظان امکان می‌دهد در هنگام وقوع حمله، به سـرعت و به طور مناسب عمل کنند.
- **قابلیت مشـاهده و کنترل** : ارائه قابلیت مشـاهده و کنترل در سـراسـر چرخه حیات حمله کامل، به محافظان کمک می‌کند تا تهدیدات را پیشگیری کنند و در صورت لزوم، اقدام سریع را هنگام وقوع حادثه فعال سازند.

آموختن از حوادث با گزارش‌های هوشمند

سان تزو می‌گوید: ***"گذشته را ببینید تا آینده را پیش‌بینی کنید."*** در امنیت سایبری:

- **گزارش‌های حوادث مبتنی بر هوش مصـنوعی** : برای محافظان مهم اسـت که بتوانند درس‌های آموخته شـده را درک کنند، اما اغلب فرآیند گزارش حوادث در مقیاس بزرگ توجه و اشتراک‌گذاری درس‌های آموخته شده را دشوار می‌سازد.
- **سـاختار اسـتاندارد** : گزارش‌های حوادث با اسـتفاده از هوش مصـنوعی تولیدی، گزارشـی ارائه می‌دهند که بررسـی مراحل انجام شده و توصیه بهبودها را آسان‌تر می‌کند. این گزارش‌ها به چهار بخش تقسیم می‌شوند (خلاصه اجرایی، خلاصه حوادث، خلاصه رویداد و جدول زمانی حوادث) و می‌توانند توسط تحلیلگر ویرایش شوند.

کتاب‌های راهنمای امنیتی سفارشی

سان تزو می‌گوید: ***"عملیات نظامی باید با دقت برنامه‌ریزی شوند."*** در امنیت سایبری:

- **دسـتورالعمل‌های سـفارشـی** : کتاب‌های راهنمای عملیات امنیتی به محافظان ارائه می‌شـود که برای نیازهای منحصـر به فرد آنها سـفارشـی شـده اسـت. کتاب راهنما (Cook Book) به محافظان امکان می‌دهد وظایف را با جریان‌های کاری خودکار سفارشی کرده و سازماندهی کنند تا بهترین شیوه‌ها را پیاده کنند.
- **آمادگی پیشـینی** : داشـتن یک کتاب راهنمای آماده که می‌تواند بیرون کشـیده شـده و به سـرعت اجرا شـود، به طور مؤثری تأثیر بر عملیات تجاری را کاهش می‌دهد.

تحقیق و تحلیل برای درک حوادث

سـان تزو می‌گوید: ***"اگر جنگ را می‌شـناسـی و خود را می‌شـناسـی، نیازی به نگرانی از نتیجه صـد نبرد نیسـت."*** در امنیت سایبری:

- **تحلیل جامع** : تجزیه و تحلیل اطلاعات موجود از منابع تهدید، گزارش‌های رویداد و سـایر منابع برای تعیین آنچه اتفاق افتاده، چه زمانی و چگونه حادثه رخ داده و کدام مهاجم حمله را آغاز کرده است.

- **نمایش بصری داده‌ها** : سازماندهی داده‌ها بر اساس ویژگی‌ها، رفتارها و مشخصات در نمای گرافیکی. قرار دادن تمام این اطلاعات در زمینه مناسب، به محافظان بینشی می‌دهد که چگونه استراتژی‌های دفاعی را در آینده تطبیق دهند.
- **تحلیل آسیب‌پذیری فعال** : خواه این امر شامل انجام اسکن‌های امنیتی منظم برای یافتن نقاط ضعف، رفع پیکربندی‌های نادرست، محدود کردن دسترسی به دارایی‌های اولویت‌دار یا برخی دیگر از تاکتیک‌های پیشگیرانه باشد.

جمع‌بندی

استراتژی‌های متنوع امنیت سایبری، رویکردی چند وجهی و منسجم به دفاع سایبری است که به سازمان‌ها امکان می‌دهد از تمام ابزارها، تکنیک‌ها و منابع در دسترس خود استفاده کنند. با داشتن یک نقطه کنترل مرکزی، تیم‌های امنیتی می‌توانند بر محدودیت‌هایی مانند کمبود تخصص، زمان یا ابزار غلبه کنند و استراتژی‌های مؤثر را در سراسر چرخه حیات کامل حمله اجرا کنند.

این رویکرد متفکرانه و پیش‌دستانه کمک می‌کند تا محافظان تهدیدات را متوقف کرده و تأثیر آنها را به کارآمدترین و مؤثرترین روش کاهش دهند. با در اختیار داشتن تخصص، منابع و کارایی مقیاس‌پذیری برای اجرای استراتژی امنیت سایبری مناسب - فارغ از اینکه چه تهدیدی پیش آید - سازمان‌ها می‌توانند با اطمینان با چالش‌های امنیتی مواجه شوند.

همان‌طور که سان تزو می‌گوید: "در مبارزه، پیروزی از تنوع حاصل می‌شود." در امنیت سایبری، این به معنای داشتن طیف وسیعی از قابلیت‌های دفاعی است که می‌توانند به طور مؤثر با انواع مختلف تهدیدات مقابله کنند. این استراتژی متنوع به سازمان‌ها امکان می‌دهد:

۱. از تجربیات گذشته برای بهبود دفاع آینده بیاموزند
۲. به سرعت و با اطمینان در برابر حملات در حال انجام واکنش نشان دهند
۳. آسیب‌پذیری‌ها را قبل از بهره‌برداری مهاجمان شناسایی و برطرف کنند
۴. استراتژی‌های دفاعی خود را با تکامل تهدیدها تطبیق دهند

با این رویکرد همه‌جانبه و متنوع، سازمان‌ها می‌توانند یک گام از تهدیدات فزاینده پیچیده امروزی جلوتر باشند.

بخش نهم: هدایت عملیات سایبری (Conducting Cyber Operations)

مقدمه

بهره‌گیری از ابزارها، اطلاعات و تخصص به منظور محافظت از سازمان، کلید موفقیت در عملیات سایبری است. این رویکرد ریشه در آموزه‌های سان تزو دارد و بر اهمیت قرار دادن نیروها در موقعیت مناسب برای بهره‌برداری از مزیت تأکید می‌کند.

اصول سان تزو در هدایت عملیات سایبری

سان تزو در فصل ۹ کتاب هنر جنگ، "ارتش در حال حرکت"، بر اهمیت جابجایی نیروها به موقعیت مناسب برای بهره‌برداری از مزیت در برابر دشمن تأکید می‌کند. او می‌گوید: ***"مزیت نظامی، مانند آب جاری است که از بلندی‌ها دوری می‌کند و به سمت پستی‌ها می‌رود".***

در عرصه نظامی، این به معنای "عملیات" است و در دنیای امنیت سایبری نیز همین اصل کاربرد دارد. اصل ۹ در "هنر دفاع" تأکید می‌کند که کلید هدایت موفق عملیات سایبری، بهره‌گیری از ابزارها، تخصص و منابع به گونه‌ای است که به محافظان مزیتی نسبت به مهاجمان می‌دهد.

چالش مدیریت منابع در محیط پیچیده

سان تزو می‌گوید: ***"فرمانده ماهر نیروهای خود را به گونه‌ای می‌چیند که پیروزی اجتناب‌ناپذیر باشد."*** در امنیت سایبری مدرن:

- **گسترش سطوح تهدید** : تحول دیجیتال، سطوح تهدید را گسترش داده و دنیای دیجیتال را پیچیده‌تر و چالش‌برانگیزتر برای ایمن‌سازی کرده است. ده‌ها ابزار، چندین تیم و انبوهی از رویکردها برای شناسایی تهدیدات، توقف حملات و کاهش خطر برای سازمان وجود دارد.
- **مشکل مقیاس‌پذیری** : بهره‌گیری از این منابع به شکل درست بسیار دشوار است، به ویژه در مقیاس بزرگ. این نیازمند آگاهی موقعیتی از محیط‌های دیجیتال و چشم‌انداز تهدید است، همچنین توانایی بسیج منابع مناسب برای اجرای استراتژی امنیت سایبری.

مثال عملی: یک سازمان مالی بزرگ با بیش از ۲۰ ابزار امنیتی مختلف و سه تیم امنیتی جداگانه، هنگام مواجهه با یک حمله هماهنگ شده، با تأخیر قابل توجهی در شناسایی و پاسخ مواجه شد. تیم‌ها به صورت جداگانه کار می‌کردند و اطلاعات حیاتی را به اشتراک نمی‌گذاشتند. با پیاده‌سازی یک مرکز فرماندهی مرکزی که داده‌ها را از تمام ابزارها جمع‌آوری و تحلیل می‌کرد، آنها توانستند زمان تشخیص را ۶۵٪ کاهش دهند و هماهنگی بین تیم‌ها را به طور قابل توجهی بهبود بخشند.

مدیریت کارآمد منابع امنیت سایبری

سان تزو می‌گوید: ***"جنگجوی برتر ابتدا پیروز می‌شود، سپس به جنگ می‌رود."*** در امنیت سایبری:

- **مدیریت منابع براساس ریسک** : راهنمایی محافظان برای مدیریت کارآمد منابع امنیت سایبری - از جمله پرسنل، بودجه و فناوری - برای اطمینان از محافظت از دارایی‌های بحرانی بر اساس ارزیابی ریسک.

- **انعطاف‌پذیری در پاسخ به حوادث** : امنیت سایبری نیازمند انعطاف‌پذیری در پاسخ به حوادث است، بنابراین برنامه‌های پاسخ به حوادث باید با انواع مختلف حوادث قابل انطباق باشند، که به تیم‌ها امکان می‌دهد تاکتیک‌ها را بر اساس نوع حمله یا انگیزه مهاجم مستقر کنند.

اجرای استراتژی امنیتی با آگاهی موقعیتی

سان تزو می‌گوید: ***"بدانید کی و کجا نبرد خواهید کرد، و شما می‌توانید با نیروهای نامحدود مقابله کنید."*** در امنیت سایبری:

- **آگاهی موقعیتی و کنترل مرکزی** : اجرای موفق استراتژی امنیت سایبری به توانایی محافظ در ارزیابی وضعیت، استقرار منابع مناسب و انجام اقدام مناسب بستگی دارد. این امر با ارائه آگاهی موقعیتی، ابزارها و یک نقطه کنترل مرکزی محقق می‌شود.
- **تقویت تخصص محافظان** : تقویت تخصص محافظان با اطلاعات تهدید مرتبط و نظارت مداوم در یک معماری باز که به آنها امکان می‌دهد در زمان و مکان مناسب اقدام درست را انجام دهند.

نظارت مداوم برای آگاهی محیطی

سان تزو می‌گوید: ***"دشمن را بشناس و خود را بشناس؛ در صد نبرد خطری متوجه تو نخواهد بود."*** در امنیت سایبری:

- **آگاهی وضعیتی و محیطی** : نظارت مداوم، آگاهی وضعیتی و محیطی را برای محافظان فراهم می‌کند، همراه با امتیاز ریسک که فوریت را مشخص می‌کند و بر اولویت‌بندی حوادث تأثیر می‌گذارد.
- **طبقه‌بندی بصری حوادث** : طبقه‌بندی بصری حوادث با استفاده از رنگ و ارائه زمینه ارزشمند برای محافظان که به توضیح نوع، تکنیک و موقعیت در محیط دیجیتال کمک می‌کند.

تحقیق و بررسی هوشمند

سان تزو می‌گوید: ***"اگر دشمن را بشناسی و خود را بشناسی، پیروزی تو قطعی است."*** در امنیت سایبری:

- **تأیید حملات** : بررسی و تحلیل اطلاعات برای تأیید وقوع حمله، تعیین سیستم‌های در معرض خطر و ارائه توصیه‌های راهنمایی شده با هوش مصنوعی برای اقدامات بعدی بهینه.
- **پاسخ غیر مخرب** : این اقدام به پاسخ سریع و غیرمخرب کمک می‌کند - خواه انجام اقدام تأیید شده یا ارجاع وضعیت به متخصص خاص برای بررسی بیشتر.

یکپارچه‌سازی و نقطه کنترل مرکزی

سان تزو می‌گوید: ***"سرعت، جوهره جنگ است."*** در امنیت سایبری مدرن:

- **راه‌حل باز و یکپارچه** : داشتن راه‌حل باز که به عنوان نقطه کنترل مرکزی برای محافظان عمل می‌کند. یکپارچه‌سازی قابلیت مشاهده و کنترل از ده‌ها ابزار امنیتی، خواه از یک فروشنده واحد یا فروشندگان متعدد، در یک مکان واحد.

- **بسیج منابع** : این به محافظان امکان می‌دهد منابع مناسب را بسیج کنند، اقدام سریع انجام دهند و در صورت لزوم تطبیق یابند. این یکپارچه‌سازی‌ها نقاط پایانی، ایمیل، شبکه، ابر، اطلاعات تهدید، برنامه‌ها و هویت را پوشش می‌دهند.

جمع‌بندی

اجرای موفق یک استراتژی امنیت سایبری به توانایی محافظ در ارزیابی وضعیت، استقرار منابع مناسب و انجام اقدام مناسب پیش از تأثیرگذاری تهدیدات مخرب بر عملیات کسب‌وکار بستگی دارد.

یک مرکز کنترل مرکزی برای محافظان، امکان هدایت عملیات سایبری را به مؤثرترین و کارآمدترین شکل بر اساس نیازهای سازمان آنها فراهم می‌کند. این رویکرد یکپارچه و جامع، به سازمان‌ها امکان می‌دهد:

۱. منابع امنیتی خود را به طور استراتژیک مدیریت کنند
۲. به سرعت تهدیدات را شناسایی و ارزیابی کنند
۳. پاسخ‌های مناسب را هماهنگ کنند
۴. از حوادث برای بهبود دفاع در آینده بیاموزند

همان‌طور که سان تزو می‌گوید: "جنگجوی برتر، جنگ را با مقاصد سیاسی می‌برد." در امنیت سایبری، این به معنای نگاه راهبردی به عملیات است - مدیریت منابع، ابزارها و افراد به گونه‌ای که نه تنها به تهدیدات کنونی پاسخ دهد، بلکه سازمان را برای چالش‌های آینده نیز آماده سازد.

با مدیریت مؤثر عملیات سایبری، سازمان‌ها می‌توانند محیط امنیتی خود را از حالت واکنشی به حالت پیشگیرانه تغییر دهند و بر پیچیدگی فزاینده چشم‌انداز تهدید غلبه کنند.

بخش دهم: پیمایش زمین سایبری (Navigating Cyber Terrain)

مقدمه

محافظانی که درک کاملی از دارایی‌های دیجیتال خود و رفتارهای تهدید دارند، می‌توانند برنامه‌های اقدامی برای مقابله با حملات را بهتر آماده کنند. این اصل برگرفته از فصل دهم کتاب هنر جنگ سان تزو است که بر اهمیت آگاهی از میدان نبرد تأکید می‌کند.

اصول سان تزو در پیمایش زمین سایبری

سان تزو در فصل ۱۰ کتاب هنر جنگ، اهمیت آگاهی از میدان نبرد را برجسته می‌کند. او می‌گوید: ***"آن که تنگناها و راه‌های گریز را می‌شناسد، پیروز می‌شود."*** ژنرالی که زمانی نیروهایش آماده حمله هستند، تشخیص می‌دهد دشمنانش کی آسیب‌پذیر هستند، و می‌تواند از زمین اطراف خود برای انتخاب میدان نبرد استفاده کند، هرگز شکست نخواهد خورد.

در دنیای امنیت سایبری، این به معنای درک کامل دارایی‌های دیجیتال خود و قابلیت‌های دشمنان، و همچنین توانایی اجرای برنامه‌های اقدام آماده شده در هنگام حمله است. رهبر امنیتی که بتواند هر سه این اهداف را تضمین کند، اطمینان خواهد داشت که می‌تواند از سازمان خود محافظت کند.

اهمیت "آگاهی موقعیتی" در محیط دیجیتال

سان تزو می‌گوید: ***"کسی که می‌داند کجا و چه زمانی می‌جنگد، پیروز خواهد شد."*** در امنیت سایبری:

- **محیط پیچیده و نامطمئن** : دنیای سایبری توزیع‌شده، پیچیده و اغلب نامشخص است. محافظانی که واقعاً "آگاهی موقعیتی" خود را در یک محیط دیجیتال درک می‌کنند - از جمله شبکه‌ها، سیستم‌ها، دامنه‌ها و داده‌ها - مزیت بزرگی در تقویت وضعیت‌های امنیتی و کاهش تأثیر حملات دارند.
- **ارزیابی ریسک و شناسایی شکاف‌ها** : رویکرد جامع و دسترسی به محافظان امکان می‌دهد ریسک را ارزیابی و شناسایی کنند، شکاف‌ها را ببندند و برنامه‌های دفاعی را برای سناریوهای مختلف حمله آماده کنند.

مثال عملی: یک شرکت تولیدی با درک عمیق از شبکه خودکارسازی صنعتی (ICS) خود، توانست آسیب‌پذیری‌های حیاتی را در نقاط اتصال با شبکه اداری شناسایی کند. با شناخت دقیق تجهیزات، نرم‌افزارها و گذرگاه‌های ارتباطی خود، آنها توانستند سیستم‌های حیاتی را با لایه‌های اضافی امنیت تقویت کنند و از یک حمله هدفمند که صنایع مشابه را هدف قرار داده بود، جلوگیری کنند.

بینش عمیق در دارایی‌های دیجیتال

سان تزو می‌گوید: ***"شناخت زمین، معرفت به آسمان است."*** در امنیت سایبری:

- **قابلیت مشاهده جامع** : بینش عمیق به دارایی‌های دیجیتال به محافظان دید روشنی از دارایی‌های دیجیتال خود می‌دهد - از جمله نوع سیستم عامل، مکان، کاربران، پروفایل‌های دارای امتیاز، حساب‌های مشترک، حساب‌های محلی، سیستم‌های متصل، آسیب‌پذیری‌های بالقوه و در نهایت، ریسک آشکار آنها برای سازمان.

- **ارزیابی ریســـک و اولویت‌بندی** : این را می‌توان با ارزش دارایی و کاربر ترکیب کرد تا به محافظان کمک کند بفهمند چه چیزی در معرض خطر است و چگونه، تا بتوانند تخصیص مناسب منابع امنیتی را اولویت‌بندی کنند.

هوشمندی تهدید برای درک دشمن

سان تزو می‌گوید: ***"اگر دشمن و خود را بشناسی، در صد نبرد خطری متوجه تو نخواهد بود."*** در امنیت سایبری:

- **بینش در تهدیدات فعلی** : هوشمندی تهدید به محافظان بینش ارزشمندی درباره تهدیدات فعلی، انگیزه‌های آنها و ابزارها و تکنیک‌هایی که معمولاً برای رساندن بار مخرب خود، تصرف سیستم‌ها یا خارج کردن داده‌ها استفاده می‌کنند، می‌دهد.
- **منابع متعدد اطلاعاتی** : این اطلاعات از منابع متعدد اطلاعات تهدید از جمله منابع داخلی محافظ جمع‌آوری می‌شود. قابلیت‌های هوشمندی و تحقیق، پیش‌بینی تهدید و پاسخ را بهبود می‌بخشد.
- **امتیازهای ریسک انطباق‌پذیر** : زنجیره‌های حمله، قوانین دارایی و امتیازات ریسک، اقدامات امنیتی انطباق‌پذیر را در سراسر چرخه حیات حمله تسهیل می‌کنند، بهینه‌سازی تخصیص منابع و هزینه در برابر ریسک واقعی.

کتاب‌های راهنما و خودکارسازی برای پاسخ سریع

سان تزو می‌گوید: ***"سرعت، جوهره جنگ است."*** در امنیت سایبری:

- **اقدام ســریع برمبنای آگاهی** : محافظان می‌توانند از این آگاهی از محیط دیجیتال خود و دانش عمیق از امضـای تهدیدات برای آماده‌سازی کتاب‌های راهنما استفاده کنند تا در صورت حمله، اقدام سریع انجام دهند.
- **پاسخ‌های خودکار متمرکز** : این کتاب‌های راهنما می‌توانند بر آسیب‌پذیری‌های شناخته شده‌ای که ممکن است مهاجم سعی در بهره‌برداری از آنها داشته باشد، متمرکز شوند و پاسخ‌های خودکاری ایجاد کنند که می‌توانند توسط یک حادثه خاص فعال شوند.
- **اقدامات متقابل فعال** : کاربردهای پیشـــرفته‌تر امکان اقدامات متقابل فعال را فراهم می‌کنند که می‌توانند برای کاهش و کند کردن پیشرفت مهاجم به کار گرفته شوند، مانند خارج کردن سیستم‌ها از شبکه، تغییر گذرواژه‌ها یا آغاز نسخه پشتیبان.

مزیت جامع محافظان

سان تزو می‌گوید: ***"ارتشی که موقعیت خود را می‌داند، پیروز خواهد شد."*** در امنیت سایبری:

- **مزیت قاطع نسـبت به مهاجمان** : محافظانی که درک جامعی از محیط‌های دیجیتال خود و ترکیب تهدید و رفتار دارند، مزیت بزرگی نسبت به مهاجمان خود دارند.
- **عملیات کارآمد** : با دانستن دارایی‌هایی که آسیب‌پذیرترین هستند و اینکه کدام تهدیدات این ضعف‌ها را هدف قرار می‌دهند، محافظان می‌توانند با اولویت‌بندی مؤثر اهداف امنیتی، تخصـــیص کارآمد منابع و ایجاد آمادگی برای پیش‌بینی حضور تأثیر مخرب عمل کنند.

جمع‌بندی

پیمایش زمین سایبری شامل درک عمیق از دارایی‌های دیجیتال، تهدیدات بالقوه و استراتژی‌های موجود برای دفاع است. با بهره‌گیری از مزیت میدان خودی، سازمان‌ها می‌توانند:

۱. به طور مؤثر محیط‌های دیجیتال خود را مشخص و نقشه‌برداری کنند
۲. آسیب‌پذیری‌ها و نقاط حساس را شناسایی کنند
۳. تهدیدات احتمالی و تکنیک‌های آنها را درک کنند
۴. برنامه‌های دفاعی و پاسخی را پیش‌اپیش آماده کنند
۵. به سرعت و قاطعانه در هنگام شناسایی حملات اقدام کنند

همان‌طور که سان تزو می‌گوید: ***"فتح کردن دشمن بدون جنگیدن، اوج مهارت است."*** در امنیت سایبری، این به معنای ایجاد چنان آگاهی قدرتمندی از محیط خود و تهدیدات بالقوه است که بتوانید موضع دفاعی غیرقابل نفوذی ایجاد کنید که مهاجمان را پیش از تلاش برای حمله، منصرف کند.

با آگاهی موقعیتی کامل، درک عمیق دارایی‌ها و تهدیدات، و آمادگی برای اقدام سریع، سازمان‌های با نیروی امنیتی آماده می‌توانند زمین سایبری را با اطمینان پیمایش کنند و بهترین استفاده را از مزیت میدان خودی ببرند.

بخش یازدهم: موضع‌های امنیتی زمینه‌ای (Contextual Security Postures)

مقدمه

ایجاد توانایی مشاهده حملات در زمان واقعی برای ارزیابی وضعیت، استقرار اقدامات متقابل مؤثر و برنامه‌ریزی یک ضربه نهایی قطعی، اساس موضع‌های امنیتی زمینه‌ای است. این اصل از فصل یازدهم کتاب هنر جنگ سان تزو الهام گرفته است.

اصول سان تزو در موضع‌های امنیتی زمینه‌ای

سان تزو در فصل ۱۱ کتاب هنر جنگ، "نه موقعیت"، به هنرمندی نُه سناریویی را توصیف می‌کند که یک ارتش ممکن است در میدان نبرد با آن مواجه شود و مجموعه‌ای از بهترین شیوه‌ها را برای چگونگی مقابله یک ژنرال با این مانورها ارائه می‌دهد. او می‌گوید: ***"ارتشی که موقعیت‌ها را می‌شناسد، پیروز خواهد شد".***

داشتن یک برنامه استوار پیش از وقوع این شرایط، به گفته سان تزو، به ارتش کمک می‌کند تا برنامه خود را با اعتماد به نفس اجرا کند و در میدان نبرد مزیت کسب نماید.

انتقال از پیشگیری به نظارت فعال

سان تزو می‌گوید: ***"در جنگ، بهترین سیاست پیشگیری است؛ بعد از آن حمله به برنامه‌ها و سپس حمله به راهبردها."*** در امنیت سایبری:

- **آگاهی موقعیتی برای اقدام** : اصل ۱۱ در "هنر دفاع" از این فلسفه بهره می‌گیرد و به محافظان توصیه می‌کند از آگاهی موقعیتی که در فصل‌های ۱ تا ۱۰ به دست آورده‌اند، برای انتقال از حالت پیشگیری منفعل به حالت نظارت فعال استفاده کنند.
- **نظارت پنهانی** : با این حال، ضروری است که این وضعیت نظارت همچنان پنهان بماند. با عدم هشدار به مهاجمان از حضور خود با اقدامات یا اقدامات متقابل، می‌توانید به طور مؤثر حرکات آنها را زیر نظر بگیرید و تاکتیک‌ها، تکنیک‌ها و روش‌های مهاجم را بیاموزید.

مثال عملی: یک شرکت خدمات مالی با استفاده از ابزارهای نظارت پیشرفته، توانست نفوذی را در شبکه خود شناسایی کند اما به جای اقدام فوری، تصمیم گرفت فعالیت مهاجمان را زیر نظر بگیرد. این استراتژی پنهان به آنها امکان داد تا مسیرهای نفوذ مهاجمان، روش‌های پنهان‌سازی و اهداف آنها را شناسایی کنند. با این اطلاعات، آنها نه تنها این نفوذ را خنثی کردند، بلکه دفاع خود را تقویت کرده و از حملات مشابه آینده جلوگیری کردند.

واکنش به حملات پیچیده امروزی

سان تزو می‌گوید: ***"سرعت، جوهره جنگ است."*** در امنیت سایبری:

- **زمان حمله، نه احتمال آن** : دیگر مسئله این نیست که آیا حمله‌ای رخ می‌دهد، بلکه مسئله زمان وقوع آن و میزان مؤثر بودن شما در محدود کردن آسیب و اختلال در عملیات تجاری است.
- **تکنیک‌های پیچیده** : مهاجمان امروزی از تکنیک‌ها و تاکتیک‌های پیچیده‌ای استفاده می‌کنند که تشخیص نفوذ اولیه و چگونگی گسترش جانبی آن‌ها در شبکه را دشوار می‌سازد.

- **تغییر سریع نقش** : نقش محافظ، تغییر سریع از تشخیص به کاهش و در نهایت نظارت است، با استفاده از یک خط مبنای از پیش تعیین شده برای جلوگیری از تبدیل وقایع امنیتی به حوادث امنیتی عمده.

بینش‌های گسترده برای اقدام سریع

سان تزو می‌گوید: ***"کسی که مسائل را می‌شناسد، پیروز می‌شود."*** در امنیت سایبری:

- **آگاهی موقعیتی عمیق** : در سراسر "هنر دفاع"، به محافظان راهنمایی داده شده است که چگونه آگاهی موقعیتی عمیقی از محیط‌های خود، کاربران و رفتارهای آن‌ها به دست آورند و اینکه دارایی‌ها کجا آسیب‌پذیر هستند یا عملکردهای تجاری حیاتی هستند.
- **اقدام سریع با بینش عمیق** : این به محافظان امکان می‌دهد تا اقدام سریع انجام دهند و بینش‌های ارزشمندی در مورد حمله جمع‌آوری کنند - از جمله چگونگی دستیابی مهاجم به دسترسی اولیه، موقعیت فعلی آنها، سیستم‌هایی که تحت تأثیر قرار گرفته‌اند و اینکه نقض تا چه حد گسترش یافته است.
- **استقرار به موقع اقدامات متقابل** : ترکیب با تحلیل تاریخی، این بینش‌های بلادرنگ به محافظان امکان می‌دهد اقدامات متقابل مناسب را به موقع مستقر کنند و از عملکردهای تجاری حیاتی قبل از ایجاد آسیب قابل توجه توسط مهاجم محافظت کنند.

نظارت مخفیانه بر مهاجمان

سان تزو می‌گوید: ***"ظاهری به خود بگیرید که دشمن نتواند تشخیص دهد."*** در امنیت سایبری:

- **نظارت پنهان در مناطق مختلف** : تولنایی نظارت مخفیانه بر مهاجمان هنگام عبور از مناطق مختلف - از ابر تا نقطه پایانی تا منطقه نظامی (DMZ) به یک دارایی حیاتی - به محافظان امکان می‌دهد اقدامات متقابل مناسب را در زمان مناسب مستقر کنند.
- **پاسخ متناسب** : یک مثال می‌تواند کاهش اعتبار یک کاربر به خطر افتاده بدون خارج کردن کل سیستم باشد. عملیات مخفیانه کلید است و به محافظان امکان می‌دهد زنجیره حمله را زیر نظر داشته باشند و گام بعدی را پیش‌بینی کنند بدون اینکه مهاجم را از تحت نظر بودن آگاه کنند.

برچسب‌گذاری دارایی‌ها و قوانین دارایی

سان تزو می‌گوید: ***"بشناس زمین را، بشناس آب و هوا را، و پیروزی تو کامل خواهد بود."*** در امنیت سایبری:

- **مشخص کردن مناطق دفاعی** : برچسب‌های دارایی برای نشان دادن ویژگی‌های مهم دارایی‌های قابل دفاع استفاده می‌شوند - خواه آنها نقاط پایانی، شبکه‌ها، هویت‌ها یا بارهای کاری باشند - همچنین برای تنظیم ارزش‌های دارایی استفاده می‌شوند تا بدانید چه زمانی دارایی‌های حیاتی درگیر هستند.
- **درک بستر دفاعی** : محافظانی که اینها را دارند، اکنون می‌توانند دارایی‌ها را به منطقه (زمین) که به آن تعلق دارند، برچسب‌گذاری کنند. این برچسب‌های دارایی به محافظان امکان می‌دهد در طول بررسی حوادث، به سرعت بینشی در مورد منطقه‌ای که از آن دفاع می‌کنند، به دست آورند.

- **اطلاعات زمینه‌ای** : با بررسی رفتارها و ویژگی‌های دارایی، می‌توانید اطلاعات زمینه‌ای درباره زمین و محیط اطراف دارایی که در تلاش برای دفاع از آن هستید، به دست آورید.

- **تسلط کامل بر سپهر تهدیدهای سایبری**: با پیگیری مستمر و جستجو در اخبارها و مقالات حملات، محافظین اطلاعات به روز و کاملی از روشها، رویکردها و رفتارهای دشمنان سایبری خود، بدست خواهند آورد و با ایجاد بانک اطلاعاتی مناسب در درازمدت **"حافظه تاریخی"** مناسبی از الگوهای تهدید خواهند داشت.

ماشه‌های خودکار، کتاب‌های راهنما و گردش‌کارها

سان تزو می‌گوید: ***"سرعت، جوهره جنگ است؛ بهره‌گیری از عدم آمادگی دشمن، رفتن از مسیرهایی که انتظار ندارد و حمله به مناطق بدون محافظت."*** در امنیت سایبری:

- **پاسخ هماهنگ و پیچیده** : سازماندهی و ترکیب فعالیت‌ها در یک طرح جامع برای سردرگم کردن و مختل کردن مهاجمان. به عنوان مثال، ممکن است بدافزاری در حال اجرای حرکت جانبی داشته باشید و تشخیص شما حرکت جانبی را نشان دهد.

- **پاسخ چند مرحله‌ای** :کتاب راهنمای (Cook Book) شما پس از تکمیل غنی‌سازی فعال می‌شود و داده‌های ماژول قابلیت مشاهده شبکه نشان می‌دهد که **"آدرس بد"** با یک هش اجرا شده است. جریان کار شما این عدم اقدام را می‌بیند و یک بلوک هش را فعال می‌کند تا از اجرای بدافزار در نقطه پایانی جلوگیری کند.

- **سردرگمی مهاجم** : این تکنیک، با تقلید از تشخیص نقطه پایانی، مهاجم را سردرگم می‌کند. شاید آنها یک اجرایی دیگر ایجاد کنند، یا شاید از ارائه اطلاعات بیشتر در مورد قابلیت‌های خود یا زمان لازم برای حذف آنها از محیط شما دست بردارند.

استقرار ضربه نهایی

سان تزو می‌گوید: ***"وقتی راه‌های فرار دشمن بسته شده است، او تا آخرین نفس می‌جنگد."*** در امنیت سایبری:

- **کاربرد دانش تجمعی** : ده فصل اول "هنر دفاع" توضیح داده است که چگونه می‌توان از ابزارهای یکپارچه برای به دست آوردن آگاهی موقعیتی در محیط‌های خود استفاده کرد و کتاب‌های راهنمایی ایجاد کرد که می‌توانند هنگام تبدیل تهدید به حمله، اجرا شوند.

- **ارزیابی خطر و استقرار اقدامات متقابل** : توانایی هماهنگ‌سازی نظارت بر حمله در سراسر ابزارهای متعدد نظارت امنیتی به محافظان امکان می‌دهد تا خطر حمله را به درستی ارزیابی کنند و اقدامات متقابل مناسب را در زمان مناسب مستقر کنند.

- **رویکرد مخفیانه برای ضربه نهایی** : مهمتر از همه، این به محافظان امکان می‌دهد این کار را به صورت مخفیانه انجام دهند، بدون آنکه مهاجم را هشیار کنند، که به محافظان امکان می‌دهد به ارزیابی وضعیت به شکلی امن ادامه دهند قبل از وارد کردن ضربه نهایی.

جمع‌بندی

موضـع‌های امنیتی زمینه‌ای به معنای ایجاد توانایی مشـاهده و ارزیابی حملات در زمان واقعی، مسـتقر کردن اقدامات متقابل مؤثر و در نهایت برنامه‌ریزی و اجرای یک ضـربه قطعی نهایی اسـت. با هماهنگ‌سـازی آگاهی موقعیتی بلادرنگ، محافظان می‌توانند:

۱. حملات را بدون هشدار دادن به مهاجمان شناسایی کنند

۲. رفتار مهاجمان را برای درک بهتر تاکتیک‌ها، تکنیک‌ها و روش‌های آنها مطالعه کنند

۳. اقدامات متقابل هدفمند را در مناسب‌ترین زمان مستقر کنند

۴. از دارایی‌های حیاتی محافظت کنند در حالی که هنوز اطلاعات بیشتری درباره تهدید جمع‌آوری می‌کنند

۵. در نهایت، یک پاسخ قطعی و جامع را برنامه‌ریزی و اجرا کنند

همان‌طور که سـان تزو می‌گوید: "پیش‌بینی به معنای پیشـگیری اسـت." در امنیت سـایبری، این به معنای داشـتن آگاهی زمینه‌ای عمیق از محیط خود، تهدیدهای بالقوه و ابزارهای در دسترس برای دفاع است، به طوری که بتوانید نه تنها به حملات پاسخ دهید، بلکه آنها را پیش‌بینی کرده، مشاهده کنید و در نهایت بدون ایجاد هشدار زودهنگام که ممکن است باعث تغییر تاکتیک‌های مهاجم شود، آنها را خنثی کنید.

بخش دوازدهم: جنگ سایبری و امنیت تهاجمی (Cyber Warfare and Offensive Security)

مقدمه

برای کسب مزیت، به محیط خود حمله کنید تا تجربه را افزایش دهید، انطباق را نشان دهید و آمادگی را تقویت کنید. این رویکرد از فصل دوازدهم کتاب هنر جنگ سان تزو، "حمله با آتش"، الهام گرفته است که به استراتژی تهاجمی می‌پردازد.

اصول سان تزو در امنیت تهاجمی

"حمله با آتش"، فصل ۱۲ در کتاب هنر جنگ، کاملاً درباره استراتژی تهاجمی است. در حالی که امنیت سایبری ذاتاً یک موضع دفاعی دارد، مواقعی وجود دارد که انجام حرکت اول ضروری است. سان تزو می‌گوید: ***"آتش را برای حمله از بیرون به کار برید، اما در داخل، از افراد استفاده کنید که در دشمن رخنه کنند".***

اصل ۱۲ در "هنر دفاع" از این فلسفه بهره می‌گیرد، اما به محافظان توصیه می‌کند که تنها در محیط خودشان به حالت تهاجمی بروند - از طریق تمرین‌های دورمیزی و سپس پیشرفت به شبیه‌سازی مهاجم - برای آماده‌سازی و اطلاع‌رسانی درباره انعطاف‌پذیری سایبری سازمان.

فکر کردن به عنوان مهاجم

سان تزو می‌گوید: ***"برای شناخت دشمن، باید دشمن شوی."*** در امنیت سایبری:

- **تفکر قرمز و آبی** : این به شما امکان می‌دهد "قرمز و آبی فکر کنید." تیم قرمز (Red Team) یا شبیه‌سازی مهاجم، تهاجم است، و تیم آبی (Blue Team)، یادگیری دفاع است. با هم، این تمرین‌های مشترک را می‌توان "تیم بنفش" نامید.
- **فراتر از بازی موش و گربه** : امنیت سایبری لزوماً نباید یک بازی دائمی موش و گربه، پلیس و دزد باشد، و استعاره مقابله همیشه مناسب نیست. تهدیدات ظاهر می‌شوند، محافظان راهی برای توقف آن‌ها پیدا می‌کنند، تهدیدات تکامل می‌یابند و این فرآیند بی‌پایان ادامه دارد.

مثال عملی: یک شرکت فناوری با استفاده از تیم قرمز داخلی، یک عملیات شبیه‌سازی فیشینگ علیه کارکنان خود اجرا کرد. این تمرین نه تنها آسیب‌پذیری‌های فرآیندهای امنیتی را آشکار کرد، بلکه تیم امنیتی را برای واکنش بهتر به حوادث واقعی آماده ساخت. کارمندانی که در این تله افتادند، آموزش‌های هدفمند دریافت کردند، و درس‌های آموخته شده به بهبود قابل توجهی در سیستم‌های تشخیص و مقابله با فیشینگ منجر شد.

یادگیری از طریق تجربه واقعی

سان تزو می‌گوید: ***"هر چند که به همه کتاب‌ها مسلط باشی، اگر جنگ ندیده باشی، هنوز معرفت واقعی نداری."*** در امنیت سایبری:

- **ارزش تجربه واقعی** : آنچه محافظان را برجسته می‌کند، این است که یاد می‌گیرند حرکت‌های بعدی مهاجم را حدس بزنند و بدون اطلاعات کامل، پیش‌بینی کنند. این امکان می‌دهد محافظ در زمان ورود یک تهدید روز صفر - چیزی که تعداد کمی از محافظان آن را دیده‌اند - آرامش خود را حفظ کند.

- **توسعه از طریق تجربه واقعی** : بسیاری از توانایی یک محافظ در اثربخشی - پیش‌بینی اقدامات بعدی مهاجم، ارائه به موقع و مؤثر اقدامات متقابل پیشگیرانه و ردیابی حملات در حال انجام - از طریق تجربیات دنیای واقعی و تکرار توسعه می‌یابد. تجربه دنیای واقعی تنها می‌تواند از طریق دو روش به دست آید: قرار گرفتن در خط مقدم حمله یا شرکت در یک "تیم قرمز دوستانه."

خدمات جنگ‌آزمایی و شبیه‌سازی حمله

سان تزو می‌گوید: ***"در زمان صلح، برای جنگ آماده شو."*** در امنیت سایبری:

- **جنگ‌آزمایی و تیم بنفش** : سرویس‌های مدیریتی پیشرفته محافظان را با قابلیت‌های پیشرفته شکار تهدید ارائه می‌دهد. این شامل گزینه‌هایی برای جنگ‌آزمایی یا تمرین تیم بنفش از طریق سناریوهای دنیای واقعی برای اعتبارسنجی قابلیت‌های دفاعی و آماده‌سازی تیم‌های امنیتی داخلی برای حمله است.

- **سناریوهای شبیه‌سازی** : برای مثال، یک سناریوی فیشینگ می‌تواند راه‌اندازی شود که در آن یک تلاش نفوذ واقعی علیه سازمان اجرا می‌شود. سپس فرآیند تشخیص و چگونگی پاسخ نهایی تیم را مشاهده می‌کنند.

- **بازخورد و توصیه‌ها** : پس از این حمله‌های شبیه‌سازی شده، می‌توانند بازخورد و توصیه‌هایی برای بهبود ارائه دهند. این خدمات به محافظان کمک می‌کند نشان دهند که کنترل‌های امنیت سایبری آنها کار می‌کند، حوزه‌های در معرض خطر را شناسایی کنند و اعضای تیم را در پاسخ‌های مؤثر آموزش دهند و تجربیات دنیای واقعی را ارائه دهند که محافظان می‌توانند هنگام مواجهه با یک مهاجم واقعی به آنها تکیه کنند.

ارزیابی‌های جامع امنیتی

سان تزو می‌گوید: ***"اگر خود و دشمن را بشناسی، در صد نبرد پیروز خواهی شد."*** در امنیت سایبری:

- **ارزیابی‌های پیشگیرانه** : ارزیابی‌های امنیتی فنی مجموعه‌ای جامع از خدمات پیشگیرانه را ارائه می‌دهند که برای ارزیابی انعطاف‌پذیری امنیت سایبری سازمان طراحی شده‌اند و توازنی بین تهدیدهایی که با آن مواجه هستند، احتمال تحقق این تهدیدها و تأثیر بالقوه بر عملیات ایجاد می‌کنند.

- **خدمات متنوع ارزیابی** : خدمات موجود شامل مدل‌سازی تهدید، آزمایش نفوذ، شبیه‌سازی تهدید تیم قرمز، ارزیابی‌های معماری امنیتی، ارزیابی‌های برنامه، ارزیابی‌های عملیات امنیتی، ارزیابی‌هایDevOps ، و بررسی‌های ساخت/پیکربندی است.

خدمات پاسخ به حوادث

سان تزو می‌گوید: ***"آمادگی بدون فرصت، بی‌فایده است؛ فرصت بدون آمادگی، بی‌فایده است."*** در امنیت سایبری:

- **خدمات پیشگیرانه و اضطراری** : خدمات پاسخ به حوادث مجموعه‌ای جامع از خدمات پیشگیرانه و اضطراری را ارائه می‌دهند که برای کمک به سازمان‌ها در آماده‌سازی، پاسخ و بازیابی از حوادث امنیت سایبری طراحی شده‌اند.

- **پاسخ فوری و تحلیل ریشه‌ای** : این خدمات شامل پاسخ فوری به حوادث برای مهار و کاهش تهدیدهای فعال، تحقیقات جنایی برای درک دامنه و تأثیر نقض‌ها، و تحلیل علت ریشه‌ای برای شناسایی آسیب‌پذیری‌ها و جلوگیری از وقوع مجدد آن‌ها است.

خدمات امنیتی مدیریت شده

سان تزو می‌گوید: ***"رهبر ماهر یارانی توانمند به خدمت می‌گیرد."*** در امنیت سایبری:

- **ترکیب تخصص و فناوری** : سرویس‌های مدیریت شده خدماتی را ارائه می‌دهند که از ترکیبی از تیم نخبه محققان، تحقیق‌کنندگان و پاسخ‌دهندگان بهره می‌برد. با استفاده از ابزارهای یکپارچه، مجموعه‌های ابزاری و فناوری‌های اضافی، این سرویس مدیریت شده بر تهدیدات و نقض‌های امنیتی بالقوه نظارت و پاسخ می‌دهد.
- **هوشمندی تهدید و جریان‌های کاری پیش‌تعریف شده** : تیم سرویس با استفاده از هوشمندی تهدید و جریان‌های کاری پیش‌تعریف برای تحقیق و پاسخ، تهدیدها و هشدارها را تشخیص داده، بررسی می‌کند و با توصیه‌ها یا تغییرات مناسب به آن‌ها پاسخ می‌دهد.
- **گزارش‌های تهدید و اقدامات پاسخ** : این سرویس شامل گزارش‌های سه‌ماهه تهدید توسط تیم تخصصی است که اطلاعاتی را درباره الگوهای تهدید فعلی و رویدادهای در حال رشد ارائه می‌دهد و اقدامات پاسخ هدایت‌شده‌ای را برای مهار، کاهش، اصلاح یا ریشه‌کن کردن تهدیدها ارائه می‌کند.

جمع‌بندی: جایگاه تهاجم در دفاع

تهاجم جایگاه خود را در "هنر دفاع" از طریق تمرین‌های دورمیزی، جنگ‌آزمایی، تمرین تیم بنفش و سایر تمرین‌های آموزشی که به محافظان می‌آموزد چگونه در هنگام وقوع حادثه مقابله کنند، پیدا می‌کند. هیچ جایگزین بهتری برای کسب تخصص مناسب وجود ندارد جز قرار گرفتن در معرض حملات واقعی.

عبور از این سناریوها با کمک متخصصان پشتیبان به محافظان امکان می‌دهد تا بفهمند سازمان کجا آسیب‌پذیر است و چگونه می‌توانند بهترین پاسخ را ارائه دهند - نشان دادن اینکه کنترل‌های صحیح در جای خود قرار دارند و تیم امنیتی تجربه و تخصص لازم را برای حفظ امنیت سازمان دارد.

همان‌طور که سان تزو می‌گوید: ***"فرصت بدون آمادگی هدر می‌رود."*** در امنیت سایبری، این به معنای آماده‌سازی تیم‌های خود از طریق تجربیات واقعی کنترل شده است، تا زمانی که یک حمله واقعی رخ می‌دهد، آنها نه تنها ابزارها بلکه تجربه لازم برای پاسخ مؤثر را داشته باشند. هدف نهایی رسیدن به سطحی از تخصص است که در آن محافظان می‌توانند:

۱. حرکات مهاجمان را پیش‌بینی کنند
۲. با اطمینان در شرایط نامشخص عمل کنند
۳. پاسخ‌های سریع و مؤثر ارائه دهند
۴. از هر حادثه برای تقویت دفاع آینده بیاموزند

با این آمادگی تهاجمی، سازمان‌ها می‌توانند از یک موضع واکنشی به یک موضع پیشگیرانه حرکت کنند، که باعث افزایش قابل توجه انعطاف‌پذیری امنیت سایبری آنها می‌شود.

بخش سیزدهم: اطلاعات و جمع‌آوری اطلاعات تهدید (Intelligence and Threat Information Gathering)

مقدمه

با ردیابی مخفیانه مهاجمان در سراسر زنجیره حمله برای تحلیل و پیش‌بینی رفتار آنها و انجام اقدامات قاطع، مزیت تاکتیکی قابل توجهی به دست آورید. این رویکرد از فصل پایانی کتاب هنر جنگ سان تزو درباره استفاده از جاسوسان الهام گرفته شده است.

اصول سان تزو در جمع‌آوری اطلاعات تهدید

سان تزو کتاب هنر جنگ را با فصلی درباره استفاده از جاسوسان در جمع‌آوری اطلاعات درباره دشمن به پایان می‌رساند. او می‌گوید: ***"آنچه به فرمانده روشن‌بینی می‌دهد و او را قادر می‌سازد نتیجه پیروزمندانه را تضمین کند، پیش‌دانش است".***

در دنیای امنیت سایبری، جاسوسی بسیار شبیه به رویکرد امنیتی تهاجمی است که در بخش پیشین توضیح داده شد. محافظان باید جاسوسان (نظارت و گزارش‌دهی) را در محیط خود مستقر کنند تا بدون آگاهی آنها، مهاجمان را به طور مخفیانه مشاهده کنند همانطور که در سراسر زنجیره حمله حرکت می‌کنند.

استقرار قابلیت "جاسوسی"

سان تزو می‌گوید: ***"بدون استفاده از جاسوس‌های بصیر، فرد بی‌رحم و بی‌احساس است و ناشایست رتبه فرماندهی است."*** در امنیت سایبری:

- **نظارت و گزارش‌دهی** : هنر دفاع در اصل ۱۳، "جمع‌آوری اطلاعات و اطلاعات تهدید"، محافظان را تشویق می‌کند تا قابلیت "جاسوسی" (نظارت و گزارش‌دهی) را مستقر کنند تا بتوانند مهاجمان را بدون اطلاع آنها زیر نظر بگیرند.
- **رفتار، پیش‌بینی و ضد اقدام** : این به شما امکان می‌دهد رفتار آنها را مشاهده، حرکت بعدی آنها را پیش‌بینی کنید و اقدامات متقابل را در زمان مناسب مستقر کنید.

مثال عملی: یک شرکت خدمات مالی سیستم‌های هانی‌پات (تله‌هایی که به نظر دارایی‌های ارزشمند می‌رسند) را در شبکه خود نصب کرد. وقتی یک گروه مهاجم به این سیستم‌های به ظاهر آسیب‌پذیر دسترسی پیدا کرد، تیم امنیتی به جای هشدار دادن فوری، فعالیت‌های مهاجمان را مشاهده کرد، ابزارها و تکنیک‌های آنها را شناسایی نمود و در نهایت، امنیت تمامی سیستم‌های واقعی را با همان آسیب‌پذیری‌هایی که مهاجمان قصد بهره‌برداری از آنها را داشتند، تقویت کرد.

محافظت در محیط متغیر امروزی

سان تزو می‌گوید: ***"در جنگ، پیروزی از انطباق می‌آید، نه از اجرای قوانین سفت و سخت."*** در امنیت سایبری مدرن:

- **پایان دفاع محیطی** : بارها در این کتاب گفته شد - **تهدیدات راه خود را به محیط شما پیدا خواهند کرد. مفهوم دفاع محیطی تغییر کرده است** – *به عبارت دیگر، محیط اطراف سایبری سیال، متخلخل و پویاست، و مهاجمان روز به روز ماهرتر می‌شوند.*

- **فراتر از واکنش‌های رودررو (رخ‌به رخ)** : محافظان باید تهدیدات را به سرعت تشخیص دهند و کنترل‌های امنیتی مناسب را برای به حداقل رساندن تأثیر مخرب مستقر کنند. اعمال واکنش رودررو به هر حادثه کار احمقانه‌ای است.

صبر استراتژیک برای اطلاعات بهتر

سان تزو می‌گوید: "***جنگجوی برتر آن است که مقدمات پیروزی خود را پیش از رویارویی با دشمن فراهم می‌کند.***" در امنیت سایبری:

- **انتظار، جمع‌آوری و اقدام** : در عوض، محافظان باید در کمین بنشینند، اطلاعات جمع‌آوری کنند و زمانی که زمان مناسب است، اقدام کنند. این نیازمند آگاهی موقعیتی کامل از محیط، آسیب‌پذیری‌ها و مهاجمان شماست.
- **طعمه برای گردآوری اطلاعات** : آنها را با دسترسی به اهداف نرم وسوسه کنید. بگذارید بین سیستم‌های کم‌اهمیت حرکت جانبی انجام دهند. نظاره کنید. یاد بگیرید. پیش‌بینی کنید. سپس، وقتی همه مهره‌ها در جای خود قرار گرفتند، اقدام قاطعی انجام دهید که تهدید را یکبار و برای همیشه از محیط شما ریشه‌کن کند.

مزیت دانستن حرکت بعدی مهاجم

سان تزو می‌گوید: "***آگاهی پیشینی نمی‌تواند از روح‌ها یا خدایان به دست آید، یا با تجربیات گذشته، یا از محاسبات. باید از افرادی به دست آید که دشمن را می‌شناسند.***" در امنیت سایبری:

- **مزیت تاکتیکی با پیش‌بینی** : دانستن آنچه مهاجم قبل از انجام آن می‌خواهد انجام دهد، به محافظان مزیت تاکتیکی عمده‌ای و هوشمندی لازم برای اقدام قاطعانه در زمان مهم می‌دهد.
- **یکپارچه‌سازی داده از ابزارهای متعدد** : یکپارچه‌سازی داده‌ها از مجموعه‌ای از ابزارهای جمع‌آوری اطلاعات، اما مهم‌ترین تهدید اطلاعاتی از محیط شما با مشاهده مهاجمان در عمل به دست می‌آید.
- **چالش فرآیندهای خودکار** : هیچ چیز ارزشمندتر از اطلاعات تهدید بلادرنگ که در مقابل شما آشکار می‌شود نیست، که به شما امکان می‌دهد اقدامات مهاجم را تحلیل و حرکت بعدی او را پیش‌بینی کنید. فرآیندهای خودکار ممکن است با کند کردن پردازش داده‌ها مانع این وظیفه حیاتی شوند، بنابراین باید توانایی‌های خود را برای نظارت کامل بر جریان داده‌های مهاجم ارتقا دهید.

راه‌حل‌های یکپارچه برای نظارت فعال

سان تزو می‌گوید: "***زنگوله‌ها و طبل‌ها، پرچم‌ها و پرده‌ها، وسایلی هستند که برای هماهنگ کردن گروه‌های مردم استفاده می‌شوند، به طوری که آنها به شکل واحدی عمل کنند.***" در امنیت سایبری:

- **هماهنگی ابزارهای امنیتی** : متمرکزسازی اطلاعات در یک منبع واحد و سیستم امنیت سازمانی (ES) امکان نظارت فعال بر حرکات مهاجم را فراهم می‌کند. این گذار از ایجاد تشخیص‌ها به کشف مهاجمان با ایجاد داشبوردهای نظارت بر مهاجمان است.

- **مقاومت در برابر تغییرات** : مزیت ترکیبی راه‌حل‌های امنیتی یکپارچه، توانایی ادامه نظارت در شـرایط انتقال بین ابزارهای امنیتی، ادغام‌ها، تحولات و زمانی است که حادثه‌ای رخ می‌دهد.

راه‌حل یکپارچه تشخیص تهدید و پاسخ به حوادث

سـان تزو می‌گوید: ***"اسـتراتژی بدون تاکتیک‌ها، آهسـته‌ترین مسـیر به پیروزی اسـت. تاکتیک‌ها بدون اسـتراتژی، صدای آشفتگی قبل از شکست است."*** در امنیت سایبری:

- **ارتقای تشخیص و بررسی** : سیستم‌های یکپارچه با گردآوری امنیت سازمانی، تشخیص تهدید، بررسی و پاسخ را با بیش از ده‌ها هزار تشخیص جعبه‌ای ارتقا می‌دهند که با چارچوب‌هایی مانند MITRE ATT&CK و NIST CSF 2.0 تراز شده‌اند.

- **یکپارچه‌سـازی وسـیع** : محافظان می‌توانند آنچه نیاز دارند را از طریق هزاران شـریک و برنامه دریافت کنند. این راه‌حل‌ها جریان‌های کاری امنیتی یکپارچه‌ای را در سراسر تشخیص، بررسی و پاسخ ارائه می‌دهند - با یکپارچه‌سازی صدها راه‌حل با پلتفرم SOAR و گردش‌کارهای خودکار تشخیص.

اصل نهایی: نظارت امنیتی مخفیانه

سـان تزو می‌گوید: ***"نبرد پنج عامل دارد... اولین عامل، راه اسـت؛ دومین عامل، آسـمان؛ سـومین عامل، زمین؛ چهارمین عامل، فرمانده؛ پنجمین عامل، روش و انضباط."*** در امنیت سایبری:

- **نظارت مخفیانه در سراسر چرخه حمله** : اصل نهایی در "هنر دفاع" توصیه می‌کند که محافظان نظارت امنیتی را به صورت مخفیانه انجام دهند تا حرکات مهاجمان را در سراسر چرخه حمله (قبل، حین و بعد) مشاهده کنند. این کمک می‌کند تا اطمینان حاصـل شـود که از دارایی‌های حیاتی محافظت می‌کنید، کسـب‌وکار را به عملیات عادی بازمی‌گردانید (اگر نکردید)، و به ما کمک می‌کند درس‌های آموخته شده را درک کنیم تا بتوانیم به طور مداوم بهبود یابیم.

- **خطر در مقابل اطمینان** : اجازه دادن به مهاجمان برای گردش در شبکه ممکن است ریسک‌آمیز به نظر برسد، اما اطمینانی که با داشـتن قابلیت مشـاهده کامل و آگاهی موقعیتی به دسـت می‌آید، این خطر را کاهش می‌دهد و به محافظان امکان می‌دهد نظاره، تحلیل و رفتار مهاجمان را پیش‌بینی کنند.

جمع‌بندی

دانسـتن آنچه مهاجم قصـد انجام آن را دارد، قبل از انجام آن، به محافظان مزیت تاکتیکی قابل توجهی و هوشـمندی لازم برای اقدام قاطعانه در زمان مهم می‌دهد. با استقرار قابلیت‌های نظارت مخفیانه، سازمان‌ها می‌توانند:

۱. رفتار مهاجمان را بدون هشدار دادن به آنها زیر نظر بگیرند

۲. تکنیک‌ها، ابزارها و اهداف مهاجمان را درک کنند

۳. حرکات بعدی مهاجمان را پیش‌بینی کنند

۴. در مناسب‌ترین زمان با اطلاعات کامل اقدام قاطعانه انجام دهند

همان‌طور که سـان تزو در آخرین فصـل هنر جنگ تأکید می‌کند: "تمام هنر جنگ بر فریب اسـتوار اسـت." در امنیت سـایبری مدرن، این به معنای استفاده از مهارت جمع‌آوری اطلاعات برای ایجاد یک مزیت اطلاعاتی بر مهاجمان است، به‌طوری‌که وقتی زمان اقدام فرا می‌رســـد، نه تنها بر تهدید فعلی غلبه می‌کنید، بلکه دانش خود را بهبود می‌بخشـــید تا بتوانید از حملات آینده مشابه جلوگیری کنید.

نتیجه‌گیری از کتاب "هنر جنگ" که در مقاله حاضر با عنوان "هنر دفاع سایبری" (The Art of Defense) آورده شده است.

تجربه در مقابله با تهدیدات

تجربه نشـان داده اسـت که سـازمان‌ها به یک اسـتراتژی جدید (با نگرش متحول شـده) نیاز دارند که به محافظان اجازه دهد با تهدیدات بسیار پیچیده در سراسر زنجیره حمله به عنوان یک نیروی متحد و منسجم مقابله کنند.

استراتژی پیشگیرانه یکپارچه

اجرای موفق این استراتژی پیشگیرانه نیازمند:

۱. قابلیت مشاهده دارایی‌های دیجیتال سازمان و دشمنان آن

۲. توانایی مطالعه حرکات و رفتار آن‌ها در زمان واقعی

۳. مکانیسمی برای اقدام قاطعانه به عنوان یک نیروی متحد برای خنثی کردن تهدید در نقطه مناسب

مرکز فرماندهی یکپارچه

یک مجموعه محصـولات حفاظتی یکپارچه، سـاخته شـده با بهره‌گیری از سـامانه‌های امنیتی یکپارچه و جامع، به شـما کمک می‌کند "هنر دفاع" را با ارائه یک مرکز فرماندهی مرکزی به محافظان اجرا کنید که از آن بتوانند پاسـخ پیشـگیرانه خود را هماهنگ کرده و تلاش‌ها را در سـراسـر افراد، فرآیندها و فناوری هماهنگ کنند. این به رهبران امنیتی اجازه می‌دهد مسـئولیت‌های خود را در مقیاس لازم توانمند کنند و آن‌ها را برای کار به عنوان یک نیروی واحد برای دفاع از عملکردهای حیاتی کسب‌وکار هدایت کنند - ریشه‌کن کردن و از بین بردن بازیگران مخربی که سازمان را تهدید می‌کنند.

همسویی با کسب‌وکار

همسـو کردن این تلاش‌ها با کسـب‌وکار اطمینان می‌دهد که تصـمیم‌گیرندگان می‌توانند با امنیت و اطمینان در محیط‌های رقابتی امروز فعالیت کنند.

آینده عملیات امنیتی

با تکامل راه‌حل‌های امنیتی به سمت یک پلتفرم یکپارچه، ضروری است اطمینان حاصل شود که محافظان به یک راه‌حل واحد محدود نمی‌شـوند که هوشـمندی، قابلیت مشـاهده و نتایج عملیاتی آن‌ها را محدود می‌کند. در عوض، به یک راه‌حل یکپارچه نیاز است که قابلیت مشاهده، بررسی، تشخیص و پاسخ منسجم ارائه دهد - چیزی که هنوز وجود ندارد.

آینده عملیات امنیتی متمرکز بر امنیت سایبری، عملکردها و توسعه بلوغ است که با هدف ساده‌تر، قوی‌تر و قابل سفارشی‌سازی کردن وظایف برای محیط منحصر به فرد هر سازمان همسو است.

یکپارچه‌سازی عمیق برای تاب‌آوری

مجموعه راه‌حل‌های حفاظتی یکپارچه، همراه با سـوئیت‌های امنیتی متنوع دیگر، انتخاب شـما جهت محافظت از همه حوزه‌ها خواهد بود و به شما امکان می‌دهد در برابر مهاجمان چابک باقی بمانید.