چگونه يك متخصص امنيتي شوم؟

ترجمه و ويرايش : امير حسين شريفي (Amirsh@sgnec.net)

چگونه يك متخصص امنيت اطلاعات شوم؟ كسب چه مهارت هاي امنيتي، آينده مرا تضمين مي كند؟ شايد اين سوال بسياري از مبتدي هاي امنيت اطلاعات باشد كه مي پرسند: "چه مهارت هايي من نياز دارم تا اولين شغل امنيتي خود را پيدا كنم؟" اخيرا در همين زمينه من با افراد زيادي برخورد كردم كه درباره مهارت هاي مورد نياز يك "تحليگر امنيتي تكنولوژي هاي اطلاعاتي" سوال داشتند.

واقعا اين سوال بسيار مهمي در زندگي حرفه اي يك شخص است كه من چگونه مي توانم مهارت هاي فردي خود را ارتقاء دهم. تقريبا در تمامي كسانيكه در حرفه هاي مربوط به كامپيوتر فعاليت مي كنند، يك نقطه مشترك وجود دارد. در حقيقت اينگونه نيست كه ما فقط در زمينه حرفه خود بايد اطلاعات كسب كنيم و آموخته شويم؛ ما نياز داريم كه از حرفه ها و تخصص هاي ديگر نيز در زمينه هاي مربوط به حرفه و شغل خود با خبر باشيم. در زمان ما، يك مركز تحصيلاتي متمركز هم نبود كه بخواهد تمامي مسايل امنيتي را يك جا مطرح كند. اما امروزه مراكز دانشگاهي و علمي متعددي هستند كه در زمينه "امنيت اطلاعات" به صورت تخصصي فعاليت مي كنند.

هر چند به دليل ضعف اغلب مراكز آموزش رسمي در زمينه امنيت اطلاعات، براي رسيدن به جايگاه يك "تحليلگر امنيتي" نياز به تلاش فردي بسياري است. درست است كه آوردن مهارت هاي دانشگاهي به دنياي واقعي امنيتي، به يك تحليلگر مي تواند كمك شاياني بكند، اما امروزه اين غلط است كه بگوييم يك نفر يك ترم درسي را در دانشگاه مي گذراند و تبديل به يك تحليگر امنيتي مي شود.

همه ما براي يك بار هم كه شده در رويايمان، خود را در جايگاه يك تحليلگر امنيتي قرار داده ايم و بدون آنكه كاري كرده باشيم پله هاي ترقي را بالا رفته ايم. اما در واقعيت چه؟ در واقعيت هم ما بهترين كسي هستيم كه نقاط ضعف خود را مي دانيم و به آن واقفيم و همانطور كه در بالا اشاره كردم فقط با كسب برخي مهارت ها مي توانيد آينده شغلي خود را تضمين كنيد.

آيا همه مسير ها به يك نقطه ختم مي شود؟

همه ما مي دانيم كه برخي حرفه ها از جمله مديريت سيستم (System Administrator)، متخصص سخت افزار – اشخاصيكه در زمينه نگهداري روترها، سوييچ ها و ابزارهاي ديگر تخصص دارند– و مديران پايگاههاي داده اي (Database Administrator)، تخصص هاي اصلي مشتركي با هم دارند.

بله! يك مدير سيستم كسي است كه بتواند در يك زمان تمامي كارهاي گفته شده در بالا را انجام دهد، البته به دليل آنكه در يك شركت بزرگ و يا در يك سازمان دولتي مشغول است فقط مي تواند در يك فيلد خاص فعاليت كند. بخشي از تخصص هايي كه يك مدير سيستم دارد در زير آمده است و بعد از آن خواهيم گفت كه چگونه آنها مي توانند براي يك تحليلگر امنيتي نيز مفيد باشند:

- دانش و تخصص لازم در زمينه سيستم هاي ويندوزي

- دانش و تخصص در زمينه پروتكل هاي اصلي شبكه
- مفاهيم معماري شبكه
- آشنايي با فايروال، راه حل هاي آنتي ويروس ها و برنامه هاي فيلتر محتوا(Content Filter)
- تخصص هاي لازم در زمينه مديريت پروژه

يكي از مهارتهايي كه يك مدير سيستم نياز دارد دانش و تخصص كافي در زمينه سيستم عامل هايي است كه در شبكه استفاده مي گردد. در شبكه هاي امروزي اين به معني يادگيري در زمينه سيستم هاي ويندوزي و در برخي مواقع لينوكسي و يا BSD مي باشد، زيرا تجربه به من نشان داده است كه در اغلب شبكه ها فقط ما از يك نوع سيستم عامل استفاده نمي كنيم بنابراين آشنايي با اغلب آنها لازم است. اين موضوع دقيقا همان چيزي است كه يك تحليلگر امنيتي بايد انجام دهد زيرا براي او تفاوتي بين سيستم عامل هاي مختلف وجود ندارد و او نياز دارد كه اطلاعات جامعي از كليه سيستم عامل هاي ذكر شده داشته باشد.

اگر شما مدير سيستم هاي ويندوزي باشيد حتما با پروتكل هاي NetBIOS و فولدرهاي اشتراكي ويندوز آشنايي كامل داريد زيرا كه آنها پايه اصلي فعاليت هاي ويندوز در شبكه هستند. يكي از ريسك هاي امنيتي اين سرويس ها، بي حفاظ گذاشتن آنها به دليل نداشتن كلمه عبور است. همه مديران سيستم ها مي دانند كه با استفاده از كلمه عبور مي توان امنيت را براي فولدرهاي اشتراكي در شبكه برقرار كرد. اين موضوع و دانش نيز يكي از چيزهاي عمومي است كه يك تحليلگر امنيتي بايد بداند.

داشتن دانش لازم در زمينه پروتكل هاي مورد استفاده از شبكه يكي از تخصص هاي مورد نياز براي هر مدير سيستم است. در ضمن يك مدير سيستم كسي است كه سرويس دهنده هاي وب (Web Server) را راه اندازي و پيكربندي مي كند .

دانش و تخصص لازم در زمينه خطاهاي پروتكل HTTP، چيزي است كه علاوه بر يك مدير سيستم، يك تحليلگر امنيني نيز آن را مي داند. همچنين دانستن پروسه هاي مورد نياز جهت محكم سازي يك سرويس دهنده وب جهت حفظ امنيت آن، دانش مورد نياز هر دو آنها است. اين موضوع در زمينه پروتكل FTP نيز صادق است.

هر دو پروتكل FTP و HTTP دو بخشي هستند كه بسيار مورد نفوذ و حمله كدهاي مخرب قرار مي گيرند. پس تعجبي ندارد كه داشتن تخصص لازم در زمينه اين دسته از پروتكل ها نياز اصلي يك مدير سيستم و يك تحليلگر امنيتي است.

معماري يك شبكه جزو بخش هايي است كه معمولا در شبكه هاي بزرگ مورد غفلت قرار مي گيرند و باز هم يك مدير سيستم تنها كسي است كه در اين زمينه بيشترين نگراني را دارد. با كمي پيچيدگي، يك شبكه مي تواند هم از داخل و هم از بيرون در معرض خطر باشد. داشتن DMZ امروزه در برابر تكنيك هاي حفاظتي ديگر، بسيار معمول و پيش پا افتاده است. همه اين مسايل كه درباره معماري و طراحي يك شبكه است، نياز به دانشي دارد كه مديران سيستم ها و تحليلگران امنيتي هر دو به اندازه كافي از آن بهره مند باشند.

هر شبكه بزرگ و امروزي داراي ابزارهاي مختلف امنيتي است. اين ابزارها شامل فايروال، راه حل هاي آنتي ويروس ها، فيلتركنندگان محتوا و پروكسي سرور ها مي باشد كه معمولا تمامي آنها توسط مديران سيستم ها، مديريت مي شود. تنها تفاوت يك مدير سيستم و يك تحليلگر امنيتي عمق دانش آنها درباره خروجي هاي اين ابزارها مي باشد. براي نمونه يك تحليلگر سيستم، كليه ترافيك خروجي يك فايروال را تجزيه و تحليل مي كند و مي گويد آيا هشدار هاي اين سيستم معتبر هستند يا خير. شايد فقط تعداد محدودي از مديران سيستم هستند كه با خواندن جزييات بسته هاي شبكه راحتند. اين كار نياز به زمان زيادي دارد، در حاليكه تنها چيزهايي كه مديران سيستم نياز دارند راه اندازي سيستم ، پيكربندي و نگهداري از اين ابزارهاست، اين همان دانشي است كه يك تحليلگر امنيتي نيز آن را دارا مي باشد.

مديريت پروژه بخشي است كه فقط در هنگام نياز به كار مي آيد. دانش و تخصص آن نيز براي يك مدير سيستم و يك تحليلگر امنيتي يكسان است. ره آوردهاي مديريت پروژه به هر فرآيندي كه يك نفر به عهده مي گيرد قابل اعمال است. شايد اين سوال در ذهن ايجاد شود كه چرا يك مدير سيستم نياز به دانستن اين مساله دارد؟ يك نگاهي به اموري كه در طول يك ماه مدير سيستم انجام مي دهد داشته باشيد. اين كارها از به روزرساني سيستم ها بعد از انتشار يك اصلاحيه تا ارائه يك سرويس جديد در شبكه مي باشد. شما براي انجام تمامي اين امور، به صورت ناخواسته اغلب مسايلي كه در مديريت پروژه مطرح است را انجام مي دهيد. براي نمونه به روز رساني سيستم عامل ويندوز XP به ويستا مي تواند به عنوان يك پروژه مطرح شود. طرح هاي مختلفي مطرح مي شود تا اين پروژه با موفقيت صورت پذيرد و اين همان كاري است كه يك مدير پروژه انجام مي دهد.

حال اين مساله چگونه به يك تحليلگر امنيتي ارتباط پيدا مي كند؟ اغلب مواقع يك تحليلگر امنيتي به عنوان يك مشاور عمل مي كند و در يك شركت بزرگ جهت امري همچون "تجزيه و تحليل ريسك" فعاليت مي كند. طراحي "سيستم مديريت اصلاحيه ها" نيز امري مشابه آن است و نياز به مشخص كردن وظايف جهت پيشبرد آن دارد. همانطور كه مي بينيد اين مسايل به گونه اي با هم شباهت دارند و نياز است كه يك ره آورد مشابه مديريت پروژه به آنها اعمال شود. در واقع اگر شما نخواهيد اين امور را تحت ره آوردهاي مديريت پروژه انجام دهيد، اين امور به سرعت و در بهترين حالت به سرانجام نخواهند رسيد.

مرور دوباره

حالا بديهي است كه مهارت هاي مورد نياز يك مدير سيستم، بسيار مشابه يك تحليلگر امنيتي است. برعكس اگر شما تخصص لازم در زمينه سيستم عامل هاي متفاوت، پروتكل هاي مختلف در شبكه و يا مهارت هاي مورد نياز يك مدير سيستم را نداشته باشيد نمي توانيد يك تحليلگر امنيتي خوب باشيد.

بيان وجوه اشتراكي اين دو حرفه بسيار سمبليك است. يك مدير سيستم نه تنها در زمينه عملكرد سرويس هاي ارائه شده در شبكه مهارت دارد، همچنين نگران وضعيت امنيتي آنها نيز است. شما نمي توانيد يك سيستم يا سرويس را بدون داشتن تخصص و دانش لازم درباره آن، امن كنيد. يك تحليلگر امنيتي شخصي است كه دانش گسترده اي دارد. شما مي توانيد يكي از تخصص هاي ديگر همچون "تست نفوذگري" (Penetration Testing) و يا متخصص "امنيت برنامه هاي كاربردي" (Web Application Security) را نيز به عنوان حرفه آينده خود انتخاب كنيد.

بنابراين براي تمامي مديران سيستم ها، انتخاب حرفه تحليلگر امنيتي نمي تواند دور از ذهن و بعيد باشد.