آموزش امنیت سایبری مقدماتی قسمت ۳ : حمله به مرکز آمار ایران (نسخه PDF)

تمامی کشور ها مسئول پاسخ گویی در مقابل فضای سایبری خود و متعهد به برقراری امنیت در این فضا هستند و این یکی از تکالیف دولت ها در برابر مردم کشورشان است.حدود دو سال قبل، تحلیلی تقدیم مسئولین ذیربط شد که در آن به پیش بینی حملات سایبری گروه های تکفیری پرداخته شده بود؛آن گفتار که هم اکنون بخشی از آن بر روی وب سایت پدافند غیر عامل وزارت صنعت و معدن آورده شده است لزوم چاره اندیشی و پیش گیری از وقوع این اتفاق را یادآور میشد.

چند ساعت قبل ،خبر از دسترس خارج شدن سایت ملی آمار ایران در رسانه ها پخش شد و عنوان شد که این حمله توسط شاخه سایبری گروهک داعش صورت گرفته است،و پس از آن چند منبع به اصطلاح آگاه،اعلام کردند که هیچ گونه درز اطلاعاتی از این مرکز صورت نگرفته است.

بادیدگاه حرفه ای اصولا مهاجمین سایبری،حملات خود را فاش نمیکنند مگر زمانی که بهره برداری اطلاعاتی لازم را هدف خود کرده باشند و تا پایان عملیات ، تمام تلاش خود را میکنند که حملات آنها مخفی بماند و کسی متوجه نفوذ ایشان نشود.واکاوی این امر که دسترسی مهاجمین به سایت مرکز آمار ایران از چه زمانی بوده است و مهاجمین چه اطلاعاتی را به سرقت برده اند یا نبرده اند،باشد بر عهده متخصصین فناوری اطلاعات این سازمان؛اما مسئله دیگر که جای سوال دارد آن است که اصلا چرا باید این اتفاق رخ دهد و چرا اقدامات لازم برای جلوگیری از این اتفاق قبلا صورت نگرفته است؟.

متاسفانه مسئولین،نگاه بسیارخوشبینانه ای در خصوص امنیت در فضای مجازی که یکی از چالش های اساسی در تمامی کشور های توسعه یافته و در حال توسعه میباشد،دارند؛با وجود آنکه کشور تاکنون هزینه ی بسیاری در قضایایی همچون ویروس استاکس نت،فلیوم،خونریزی قلبی و... داده است،باز هم شاهد اقدامی جدی برای مقابله با این آسیب ها نیستیم.

برخی سیاست ها همچون کم کردن بوجه نظامی و امنیتی کشور،یا بکار گیری نیروهای متخصص برای حمله به مراکز برخی کشور های متخاصم، در شرایطی که خود ما چالش های بسیار جدی در این حوزه داریم موجب شده تا از دفاع سایبری و بالا بردن درصد امنیت در مرزهای خودمان قافل شویم.

توسعه در فضای سایبری و افزایش خدمات دهی به شهروندان بی شک یکی از سیاست های دولت الکترونیک میباشد،اما در صورتی امنیت شهروندان در این بین آسیب ببیند،چه مقدار از ارزش آن کاسته خواهد شد؟آیا هم اکنون،مراکز پلیس به علاوه ده،دفاتر امور اتباع و مهاجرین که توسط بخش خصوصی اداره میشود،استاندارد های لازم برای جلوگیری از درزاطلاعات را رعایت میکنند؟سایر ارگان ها،ادارات،وزارت خانه ها،پست مرکزی،بهزیستی،اتاق های بازرگانی،نیروگاه ها و مراکز حیاتی دیگر که اطلاعات مهمی بر روی سیستم های کامپیوتری خود دارند چطور؟

در صورتی که یک کشور متخاصم قصد حمله به کشور و شهروندان کشور دیگری را داشته باشد،از مهم ترین مسائلی که باید بررسی شود این است که کشور هدف در چه سطحی قرار دارد،آیا کشوری جهان سومی است یا کشوری در حال توسعه و یا توسعه یافته؛بدون شک در صورتی که گروه های تکفیری نظیر داعش،قصد ضربه زدن به ایران را داشته باشند،

سیاست آن ها با آنچه ایشان در عراق و سوریه پیاده کردند متفاوت است؛ایران کشوری در حال توسعه میباشد و بهترین راه برای ضربه زدن یک گروهک تروریستی به چنین کشوری،حملات نامتقارن است،حملاتی که طی آن ایران ضربه میبینند اما نمیتواند در فضای مشابه مقابل به مثل کند،این ادعا وقتی تقویت میشود که خصومت یک گروهک تروریستی با کشور ما کاملا عیان است و ایشان بدون شک از هر فرصتی برای وارد کردن ضربه به ایران استفاده میکنند.

حمله اخیر میتواند یادآور این نکته باشد :هنگامی که هکرهایی با مهارت اندک قادرند دسترسی به سایت ها و مراکز مهم ما داشته باشند احتمالا- هکر های حرفه ای و سازمان یافته که از جانب کشور های متاخصم هدایت میشوند میتوانند ضربه های جدی تری به ما وارد کنند،این مطلب صحیح است که ما میتوانیم در همان فضا پاسخ درخور به این تجاوز ها بدهیم اما این امر نباید ما را از دفاع سایبری غافل کند.

به طور کلی برای حمله به اکثر شبکه های دولتی و یا بخش خصوصی ابتدا مهاجم مجبور است به اینترنت و شاهراه اطلاعاتی مراجعه کند،لذا اگر توان این را داشته باشیم که حمله را در همان ستون اصلی شبکه شناسایی کنیم،میتوانیم قبل از اینکه به شبکه حمله شود آن را

متوقف کنیم؛

لذا میبایست در ابتدا امنیت را در شاهراه اطلاعاتی برقرار کنیم؛در این زمینه مشکلات فراوانی وجود دارد که با نظر کارشناسان باید برطرف شود،از جمله این مشکلات سرعت بالا و حجم بالای ترافیک و سلب امنیت روانی از شهروندان و شائبه جاسوسی دولت از ملت میباشد؛برقراری امنیت میبایست از بالاترین تا پایین ترین سطوح یعنی حفاظت از یک رایانه شخصی ادامه پیدا کند،

میبایست همان طور که به کارخانه های سازنده اتومبیل اجازه نمیدهیم که اتومبیل بدون کمربند ایمنی تولید کنند و اکثر کشورها نیز به مردم اجازه نمیدهند بدون بستن کمربندها رانندگی کنند ،در امنیت فضای سایبری هم همین منطق دنبال شود،چرا که امنیت ضعیف رایانه هر فرد میتواند به مشکلات امنیت ملی برای همه افراد منجر شود.

متاسفانه بسیاری از نرم افزار هایی که هم اکنون بر روی لپ تاپ ها و گوشی های هوشمند نصب شده است،خود دروازه ای برای هجوم هکر ها و یا جمع آوری اطلاعات توسط ایشان میباشد،دولت ها و دستگاه های مسئول میبایست در برابر این جرائم از شهروندان خود دفاع کنند و به بهانه های مختلف نباید از آن چشم پوشی کنند.

از نکات دیگر که میباید در زمینه دفاع سایبری به آن توجه ویژه داشت،قطعات الکترونیکی است،ضعف کشور ما در قسمت تولید سخت افزار و وارداتی بودن این محصولات در اکثر موارد،خبر از تهدید بالقوه ای بر علیه فضای سایبری ماست.

متاسفانه در شرایط فعلی اکثر شرکت های خصوصی که در زمینه امنیت اطلاعات مشغول فعالیت هستند خود آرایشی امنیتی گرفته اند و نمیتوان از متخصصین و کارشناسان بسیاری که دانش قابل توجهی در این زمینه دارند،اما تمایل ندارند وارد چنین فضایی شوند استفاده کرد.

با توجه به قدرت گرفتن شاخه سایبری داعش،و حملاتی که توسط ایشان در چند ماه اخیر رخ داد نظیر هک یکی از شبکه های تلوزیونی فرانسه و همچنین بهره برداری ایشان از ابزار ها و دانش هایی که توسط اربابانشان در اختیار ایشان میگذارند، حمله به وب سایت مرکز آمار،اولین و آخرین آن نمیباشد و بنابر اهداف مهاجمان میتواند به نقاط مختلف با اهداف مختلف صورت گیرد،هزینه کم و نامتقارن بودن آن،همچنین تاثیرات روانی که بر ذهن شهروندان کشور میگذارد موجب تقویت شدن این ادعاست.

سعید طوسی

رسول دانش

سلام

حرف شما صحیحه اما مشکلاتی که من توی محیط کاری باهاش برخورد کردم اینه که امنیت معمولا آخرین موضوع قابل فکر کردن توی بخش it است و من دلیل اصلی اونو اطلاعات بسیار کم مسئولین it شرکتها راجع به مسائل امنیت سایبری است و دوستان و همکاران بخاطر اینکه توی این بخش ضعیف هستند اصلا ورود نمی کنند واصلا خطرات رو اعلام و گوش زد نمی کنند چون کار خودشون بخاطر ضعف علمی زیر سئوال میره و از اونجایی که در ایران شایسته سالاری کمه و رابطه غوغا میکنه و مسئولین it هم ازین قاعده مستثنی نیستند

این ضعف علمی بیشتره

تنها راهی که به ذهن حقیر میرسه اینه که یک آموزش کاربردی و آسان و ارزون و یک پارچه ایجاد بشه که بتونه به همه دوستان با همه سطوح علمی کمک کنه

من تا بحال آموزش یکپارچه ای و کاملی در هیچ جا ندیدم

بعضی از سایتها خیلی خوب شروع کردن اما بعد از ۲ یا ۳ جلسه یا تعطیل کردن یا منحرف شده و به حاشیه رفتن (البته نمی دونم از طرف نهادهای امنیتی تحت فشار بودن یا نه)

اینو دیدم که بعضی از سایتها به خاطر این آموزش ها فیلتر شدن اما بنظر من این پاک کردن صورت مسئله است و باید با این قبیل آموزش ها کلا یک پله سطح دانش امینیتی رو بالا برد

محمد رفیعی

سلام و عرض پوزش ، به نظر میرسه یک نکته ریز باید در این مقاله ارزشمند تصحیح بشه و اونم این که گروه تروریستی داعش مسئول این هک نبوده و یک گروه سعودی به نام داعس یا Da۳s که تحت نظر دولت سعودی فعالیت میکنه این هک را انجام داده.

سعید خانی پور قبادی

متاسفانه یکی از مشکلاتی که من باهاش خیلی برخورد می کنم مدیریت های حاج آقایی هستش که در بحث آی تی و امنیت بسیار بی اهمیت هستند

سعید طوسی

جناب رفیعی صحیح میفرمایید،در زمان نگارش مقاله،مسئول این حملات گروه نامبرده تلقی میشد؛در هر صورت هدف اصلی از نگارش این مطلب یادآوری تهدیدات نامتقارن،بر علیه فضای سایبری کشور بود.

حسین عابدین زاده

سلام

طبق عرایض جنابعالی تنها کارشناسان خبره صلاحیت تشخیص دزدی شدن اطلاعات را دارند.

مثل بلایی که سر diginotar اومد و شرکت کلا منحل شد.

معلوم نیست که چه اطلاعاتی ربوده شده و حمله تا چه سطحی صورت گرفته. اما خوب یا بد من این قبیل اتفاقات رو به فال نیک می گیرم.

چرا که تو ایران و فرهنگ ایرانی تا اتفاقی نیوفته فکر چاره ای صورت نمی گیره و با این قبیل اتفاقات عرصه برای پیشرفت شرکت های IT Base باز میشه و متخصیصین واقعی جایگاه خودشونو پیدا می کنن.

بعد از این قبیل اتفاقات هستش که شما می تونید پیشنهاد های سخت افزاری و نرم افزاری و Solution های امنیتی رو مطرح کنید.

حجت رستمی

با سلام و احترام

درابتدا ، امیدوارم از صحبتهایی که میکنم دلگیر نشوید

مقاله شما دوست عزیز رو مطالعه کردم و همچنین نظر سایر دوستان گرامی رو باید خدمت شما (نویسنده صرفا) عرض کنم که ابتدا بهتر بود این مطلب رو به عنوان یک بحث و یا یک خبر عنوان میکردید نه مقاله ، مطلبی که نوشتید از نظر فنی کمی ایراد بهش وارده که پله پله بررسی میکنم و امیدوار هستم که نتیجه گیری من رو با فرمایشات خودتون کامل کنید ... واما بعد

در مورد این مطلب که شما فرمودین : حدود دو سال قبل، تحلیلی تقدیم مسئولین ذیربط شد که در آن به پیش بینی حملات سایبری گروه های تکفیری پرداخته شده بود؛آن گفتار که هم اکنون بخشی از آن بر روی وب سایت پدافند غیر عامل وزارت صنعت و معدن آورده شده است لزوم چاره اندیشی و پیش گیری از وقوع این اتفاق را یادآور میشد. باید به عرض برسونم که مقوله امنیت دوست عزیز یک بحث مطلق نیست و کاملا نسبی هست این جمله به این معنی که هر چه در ضمینه امنیت اطلاعات شما تلاش کنید به هر هال باز امکان نفوذ وجود دارد اگر حوزه IT (فناوری اطلاعات) رو برای شما به دو دسته کلی تقسیم کنیم بخش شبکه های کامپیوتری و امنیت شبکه : در قسمت شبکه اصولا خواستن توانستن است ولی در امنیت اطلاعات خواستن توانستن نیست و بسته به فردی که در پشت سیستم برای هک قرار گرفته است برای داده های ورودی شما خروجی یکسانی وجود ندارد و علاوه بر بعد فنی که استفاده از ابزار های امنیتی میباشد ضریب هوشی و نبوغ فردی در رسیدن به پاسخ ، جوابهای متفاوتی رو برای شما به وجود خواهد آورد در صورتی که در حوزه شبکه های کامپیوتری ادمین های شبکه با یک سری نرم افزار ازپیش تعریف شده سرکار دارند که درنهایت خروجی

یکسـانی رو برای شـما به ارمغان خواهـد آورد بـدون درنظر گرفتن اینکه فرد ادمین دارای چه توانایی های فردی برای انجام فعالیتهای محوله است . بنابراین دنبال راهکار ثابت بودن برای پیشـگیری از جرم رایانه ای به عنوان راهکاری برای پیشگیری از هرگونه نفوذ کاری بیهوده است .

درخوصوص اینکه فرمودین (چنـد ساعت قبل ،خبر از دسترس خارج شدن سایت ملی آمار ایران در رسانه ها پخش شد و عنوان شد که این حمله توسط شاخه سایبری گروهک داعش صورت گرفته است،و پس از آن چند منبع به اصطلاح آگاه،اعلام کردند که هیچ گونه درز اطلاعاتی از این مرکز صورت نگرفته است.

بادیـدگاه حرفه ای اصولا مهاجمین سایبری،حملات خود را فاش نمیکننـد مگر زمانی که بهره برداری اطلاعاتی لازم را هـدف خود کرده باشـند و تا پایان عملیات ، تمام تلاش خود را میکنند که حملات آنها مخفی بماند و کسی متوجه نفوذ ایشان نشود.واکاوی این امر که دسترسی مهاجمین به سایت مرکز آمار ایران از چه زمانی بوده است و مهاجمین چه اطلاعاتی را به سرقت برده اند یا نبرده اند،باشد بر عهده متخصصـین فناوری اطلاعات این سازمان؛اما مسئله دیگر که جای سوال دارد آن است که اصلا چرا باید این اتفاق رخ دهد و چرا اقدامات لازم برای جلوگیری از این اتفاق قبلا صورت نگرفته است؟.) این قسمت از صحبت شما به شدت مغرضانه است دوست گرامی اصولاـ هـدف از حمله سـایبری همیشه به سـرقت بردن اطلاعات نیست و جنبه های فنی دیگری ماننـد ایجاد جنگ روانی بر علیه یک سازمان دولتی با اهـدافی نظیر ایجاد حس بی اعتمادی در میان مردم ، ایجاد فضای تولید خبر و هجمه رسانه ای در روزنامه ها ، برهم زدن تمرکز حکومتی برای نیـل به یـک هـدف خـاص تر و.... را شامـل میشود و اگر داده ای از این سازمان به سـرقت رفته بود مطمئن باشید که فرد متخاصم برای قدرت نمایی هم که شده تمام یا بخشی از آن را به صورت عمومی منتشر می کرد تا ضعف این سازمان در حفظ و نگهـداری از اسـناد در اختیارش را به رخ بکشـد که قطعا تاثیر بیشتری هم برایش داشت . و اینکه با اقتدار تمام گفته اید چرا اقـدامات لازم برای جلوگیری از این اتفاق قبلا صورت نگرفته است؟. مگر شـما از اقدامات صورت گرفته مطلع بوده اید که به مسـئولین سایت این سازمان ایراد گرفته و این چنین سوآل سنگینی پرسیده اید ؟؟؟

درخصوص اینکه فرمودیـد (متاسـفانه مسـئولین،نگـاه بسـیارخوشبینانه ای در خصوص امنیت در فضای مجازی که یکی از چالش های اساسـی در تمـامی کشور های توسـعه یافته و در حال توسـعه میباشـد،دارنـد؛با وجود آنکه کشور تاکنون هزینه ی بسـیاری در قضایایی همچون ویروس استاکس نت،فلیوم،خونریزی قلبی و... داده است،باز هم شاهد اقدامی جدی برای مقابله با این آسیب ها نیستیم.

برخی سیاست ها همچون کم کردن بوجه نظامی و امنیتی کشور،یا بکار گیری نیروهای متخصص برای حمله به مراکز برخی کشور های متخاصم، در شـرایطی که خود ما چالش های بسـیار جدی در این حوزه داریم موجب شده تا از دفاع سایبری و بالا بردن درصد امنیت در مرزهای خودمان قافل شویم.)

شما این قسـمت رو طوری نوشتید که گویی عضوی از مجلس شورای اسـلامی یا یک مقام بلند پایه درسـطح شورای عالی امنیت ملی هستید . اول اینکه مگر شما از بودجه دفاعی کشور که امری محرمانه میباشد اطلاع دارید که اگر اینطور است از کجا آورده اید (خوش به هـالتون که داریـد) دوما در مورد حملات سایبری که گفتیـد با بکار گیری نیروهای متخصـص برای حمله به مراکز برخی کشور های متخاصم،میشه از این حملات به صورت موردی که به تایید مقامات امنیتی کشور و یا هر مسـئول دولتی دیگر رسیده است و به صورت عمومی منتشـر شده مثال هایی رو ذکر کنید که این جان برکف ها به کدام سایت و سازمان حمله کرده اند که شـما از آن یاد کرده اید این در هالی است که فعلا ما در مجامع بین المللی تاوان کارهای انجام نـداده را میـدهیم چه رسـد به اینکه چنین حمله تکنولوژیکی را نیز انجام دهیم که فکر کنم بیایند و دور تا دور ایران را دیوار بتونی با سـیمان تیپ ۵ بریزند . خوب بود از روی احساسات هیچ ضعفی را قضـاوت نمی کردیـد و اینچنین عملکرد دیگران را زیر سوآل نمی بردی که کـاری بس نکوهیـده است و داشـتن ضن و گمان بـد به دیگران در هالی که هیچ اطلاعی از عملکر آن گروه نداریم میشود بیان امیرالمومنین

مَن لَم یُحسِن ظَنَّهُ استَوحَشَ مِن کُلِّ أَحَدٍ؛

آن کس که گمان خود را نیکو نسازد (و بدبین باشد) از هر کسی وحشت می کند.(تصنیف غررالحکم و دررالکلم ص ۲۵۴)

اَلمُریبُ اَبَدا عَلیلٌ؛

آدم بدبین، همیشه بیمار است.(تصنیف غررالحکم و درر الکلم ص ۷۲)

درمورد این قسـمت (توسـعه در فضای سایبری و افزایش خدمات دهی به شـهروندان بی شک یکی از سـیاست های دولت الکترونیک میباشد،اما در صورتی امنیت شـهروندان در این بستر آسـیب پـذیر چه مقدار از اینش آن کاسته خواهد شد؟آیا هم اکنون مراکز پلیس به

علاوه ده،دفاتر امور اتباع و مهاجرین که توسط بخش خصوصی اداره میشود،استاندارد های لازم برای جلوگیری از درزاطلاعات را رعایت میکنند؟سایر ارگان ها،ادارات،وزارت خانه ها،پست مرکزی،بهزیستی،اتاق های بازرگانی،نیروگاه ها و مراکز حیاتی دیگر که اطلاعات مهمی بر روی سیستم های کامپیوتری خود دارند چطور؟) الله وکیلی اگه خبر BBC تست خبر نگاری بدی رو هوا میبرنت : در طرح سوآلاتی که باعث از بین رفتن حس اعتماد و ایجاد شک نسبت به ارگانهایی که رسما ازشون نام بردی مهارت و نبوغ خاصی داری

درخصوص اینکه گفتید (در صورتی که یک کشور متخاصم قصد حمله به کشور و شهروندان کشور دیگری را داشته باشد،از مهم ترین مسائلی که باید بررسی شود این است که کشور هدف در چه سطحی قرار دارد،آیا کشوری جهان سومی است یا کشوری در حال توسعه و یا توسعه یافته؛بدون شک در صورتی که گروه های تکفیری نظیر داعش،قصد ضربه زدن به ایران را داشته باشند،سیاست آن ها با آنچه ایشان در عراق و سوریه پیاده کردند متفاوت است؛ایران کشوری در حال توسعه میباشد و بهترین راه برای ضربه زدن یک گروهک تروریستی به چنین کشوری،حملات نامتقارن است،حملاتی که طی آن ایران ضربه میبیند اما نمیتواند در فضای مشابه مقابل به مثل کند،این ادعا وقتی تقویت میشود که خصومت یک گروهک تروریستی با کشور ما کاملا عیان است و ایشان بدون شک از هر فرصتی برای وارد کردن ضربه به ایران استفاده میکنند.) این بیان مشخص میکنه که شما اصلا از قدرت امنیتی ایران هیچ اطلاعی ندارید دوست عزیز سیاست راهبردی ایران در دفاع تعریف شده نه در حمله که به مقابله به مثل در فضای متقابل ختم بشه دوست عزیز کشوری که متخصصان اون در فرماندهی پدافند دفاع غیر عامل امکان هک کردن هواپیماهای پیشرفته ای نظیر RQ۱۷۰ رو دارند و اون رو سالم شکارش میکنند اگر اراده کنند در همون فضای مشابه که فرمودین برای مقابله به مثل حرفهای زیادی برای گفتن دارند . (به قول برو بچ اسلام دست و پاشون رو بسته) نمی دونم چرا همش تلاش کردی ایران رو و متخصصان اون رو ضعیف جلوه بدی

در خصوص اینکه فرمودین (حمله اخیر میتواند یادآور این نکته باشد :هنگامی که هکرهایی با مهارت اندک قادرند دسترسی به سایت ها و مراکز مهم ما داشته باشند احتمالا هکر های حرفه ای و سازمان یافته که از جانب کشور های متاخصم هدایت میشوند میتوانند ضربه های جدی تری به ما وارد کنند،این مطلب صحیح است که ما میتوانیم در همان فضا پاسخ درخور به این تجاوز ها بدهیم اما این امر نباید ما را از دفاع سایبری غافل کند.) ببخشین یه سوآل ازتون دارم شما مهارت هکر های متجاوز رو با چه سنگ محکی سنجیدی که گفتین با این مهارت اندک به سازمانهای ما حمله می کنند مگر شما از تجهیزات نصب شده در این سازمان آمار اطلاع دارید که از چه نوع فایروالهایی به طور مثال استفاده می کنند .یا با خود این هکر ها صحبت کردید و فهمیدید غیر حرفه ای هستند و.... وای به هال ما اگر متخصصان حرفه ای شون مثلا حال کنند فردا صبح به ما حمله کنند چه کنیم . (خوب چرا اینقدر جو الکی میدی)

در مورد (به طور کلی برای حمله به اکثر شبکه های دولتی و یا بخش خصوصی ابتدا مهاجم مجبور است به اینترنت و شاهراه اطلاعاتی مراجعه کند،لذا اگر توان این را داشته باشیم که حمله را در همان ستون اصلی شبکه شناسایی کنیم،میتوانیم قبل از اینکه به شبکه حمله شود آن را متوقف کنیم؛لذا میبایست در ابتدا امنیت را در شاهراه اطلاعاتی برقرار کنیم؛در این زمینه مشکلات فراوانی وجود دارد که با نظر کارشناسان باید برطرف شود،از جمله این مشکلات سرعت بالا و حجم بالای ترافیک و سلب امنیت روانی از شهروندان و شائبه جاسوسی دولت از ملت میباشد؛برقراری امنیت میبایست از بالاترین تا پایین ترین سطوح یعنی حفاظت از یک رایانه شخصی ادامه پیدا کند،میبایست همان طور که به کارخانه های سازنده اتومبیل اجازه نمیدهیم که اتومبیل بدون کمربند ایمنی تولید کنند و اکثر کشورها نیز به مردم اجازه نمیدهند بدون بستن کمربندها رانندگی کنند ،در امنیت فضای سایبری هم همین منطق دنبال شود،چرا که امنیت ضعیف رایانه هر فرد میتواند به مشکلات امنیت ملی برای همه افراد منجر شود.

متاسفانه بسیاری از نرم افزار هایی که هم اکنون بر روی لپ تاپ ها و گوشی های هوشمند نصب شده است،خود دروازه ای برای هجوم هکر ها و یا جمع آوری اطلاعات توسط ایشان میباشد،دولت ها و دستگاه های مسئول میبایست در برابر این جرائم از شهروندان خود دفاع کنند و به بهانه های مختلف نباید از آن چشم پوشی کنند.) اینکه راهکار ارائه کردین پسندیده است و از نظر فنی قابل بررسی من هم می پسندم حرفتون رو اما اما ایجاد اجبار برای حفظ اصول امنیت در رایانه های شخصی ورود به حریم خصوصی محسوب میشه عین این هست که من به شما بگم آقا از این به بعد خودروی شما در داخل حیاط منزلتون هم باید قفل فرمون و پدال هم باید داشته باشه خوب غیر منطقیه درستش این هست که آموزش های لازم در این رابطه به مردم اطلاع رسانی بشه حق انتخاب با خودشون باشه بهتره یادمون باشه از ابزار قانون چماق نسازیم ، زندانی نسازیم که خودمون در آن گیر بیفتیم رعایت نکردن اصول امنیتی جرم محثوب نمیشه و هر خطری هم که به بار آورد متوجه خود فرد است (جامعه شهری و انسانی پادگان نظامی نیست که اصول حفظ امنیت اطلاعات با گارد نظامی قابل حل باشه و نیاز به فرهنگ سازی در استفاده از فناوری اطلاعات داره) جامعه و حکومت رو در مقابل هم قرار ندیم در کنار هم مشکلاتی از این دست قابل حل است .

این جمله که گفتین :از نکات دیگر که میباید در زمینه دفاع سایبری به آن توجه ویژه داشت،قطعات الکترونیکی است،ضعف کشور ما در قسمت تولید سخت افزار و وارداتی بودن این محصولات در اکثر موارد،خبر از تهدید بالقوه ای بر علیه فضای سایبری ماست. کاملا صحیح و حق با شماست

این که گفتین (متاسفانه در شرایط فعلی اکثر شرکت های خصوصی که در زمینه امنیت اطلاعات مشغول فعالیت هستند خود آرایشی امنیتی گرفته اند و نمیتوان از متخصصین و کارشناسان بسیاری که دانش قابل توجهی در این زمینه دارند،اما تمایل ندارند وارد چنین فضایی شوند استفاده کرد.

با توجه به قدرت گرفتن شاخه سایبری داعش،و حملاتی که توسط ایشان در چند ماه اخیر رخ داد نظیر هک یکی از شبکه های تلوزیونی فرانسه و همچنین بهره برداری ایشان از ابزار ها و دانش هایی که توسط اربابانشان در اختیار ایشان میگذارند، حمله به وب سایت مرکز آمار،اولین و آخرین آن نمیباشد و بنابر اهداف مهاجمان میتواند به نقاط مختلف با اهداف مختلف صورت گیرد،هزینه کم و نامتقارن بودن آن،همچنین تاثیرات روانی که بر ذهن شهروندان کشور میگذارد موجب تقویت شدن این ادعاست.)

اتفاقا متخصصین امنیت اطلاعات در این حوزه خیلی هم خوب کار میکنند رعایت ممیزی امنیت اطلاعات در هر کشوری از سوی سازمان های امنیتی برای کنترل و پیش گیری جرایم دال بر پاک کردن صورت مسئله نیست . از گروهک تروریستی داعش نباید غافل شد ولی از این گروه غول بی شاخه دم هم نسازید قابل کنترل و نابودی است . دشمنان ایران هرگز درخواب نمی روند و ما متخصصین ما هم در مراجع قانونی ایشالله بیدار هستند .

موفق باشید .

سعید طوسی

#hojat.rostami

سلام،ممنون از اینکه مقاله رو با دقت خوندین،و اما پاسخ

اول اینکه بنده هیچ جا مدعی نشدم که امنیت مساله مطلق است،و مسئله ای که فرمودید احتمالا بازتاب قلم ضعیف بنده است که موجب شده خواننده چنین برداشتی داشته باشه.

و بعد:بنده اگر قصد نقد مغرضانه داشتم،به نحو دیگری قلم میزدم،بنده ادعا کردم اقدامات کافی برای محافظت انجام نشده ،به این مطلب در بیانیه ای که توسط پلیس فتا انتشار یافته هم اشاره شده است،دیفیس شدن یک سایت دولتی(فرق نمیکند متعلق به سازمان آمار باشد یا وزارت خارجه یا ارشاد)،از نظر بنده فاجعه ست،اما اگر نظر شما عزیزان ایراد بزرگی نیست به همین شیوه خود ادامه دهید.

فرمودید:(شما این قسمت رو طوری نوشتید که گویی عضوی از مجلس شورای اسلامی یا یک مقام بلند پایه درسطح شورای عالی امنیت ملی هستید . اول اینکه مگر شما از بودجه دفاعی کشور که امری محرمانه میباشد اطلاع دارید که اگر اینطور است از کجا آورده اید (خوش به هالتون که دارید) دوما در مورد حملات سایبری که گفتید با بکار گیری نیروهای متخصص برای حمله به مراکز برخی کشور های متخاصم،میشه از این حملات به صورت موردی که به تایید مقامات امنیتی کشور و یا هر مسئول دولتی دیگر رسیده است و به صورت عمومی منتشر شده مثال هایی رو ذکر کنید که این جان برکف ها به کدام سایت و سازمان حمله کرده اند که شما از آن یاد کرده اید این در هالی است ...)

بنده تعجب میکنم از این الفاظ،باید به خدمتتان عرض کنم،بودجه دفاعی و نظامی تماما محرمانه نیست،ثانیا گزارشات کمیسیون امنیت ملی مجلس و همچنین گزارشات و اخباری که از سایر نهاد های دفاعی بیرون میآید میتواند راهگشا برای محققین باشد!

همین چند هفته پیش عکس هفت جوان ایرانی در آمریکا بالا برده شد و ایشان تحت پیگرد نهاد های امنیتی این کشور قرار گرفتند به جرم نفوذ به شبکه های رایانه ای!

بنده تکذیب این خبر را ندیدم،اگر شما مطلعید بفرمایید

بنده به سیاست استفاده از جوانان نخبه ایرانی برای حمله به مراکز حساس کشور های متخاصم،در شرایط فعلی نقد جدی دارم.

چند شب پیش ۴۱۸ سایت ایرانی توسط یک جوجه هکر عربستانی ،از دسترس خارج شد

وب سایت وزارت امورخارجه از دسترس خارج شد

وب سایت وزارت ارشاد از دسترس خارج شد

و دوباره میگویم،اگر این سطح امنیت از نظر مسئولین مورد تایید است،ادامه بدهند به سیاست های فعلی...

و باز فرمودیـد: الله وکیلی اگه خبر BBC تست خبر نگـاری بـدی رو هوا میبرنت : در طرح سوآلاتی که باعث از بین رفتن حس اعتماد و ایجاد شک نسبت به ارگانهایی که رسما ازشون نام بردی مهارت و نبوغ خاصی داری...

در خصوص مراکزی که عرض کردم،چون حساس هسـتند،نمیتوانم اطلاعات چنـدانی بـدهم،در مقاله هم خیلی سـریع از این بخش رد شدم.

اما اگر گمان میکنید این مراکز امن هستند،باز هم رویه فعلی را دنبال کنید...

فرمودید سـعی در این داشـتم که ایران و متخصصان آن را ضعیف جلوه بدهم؛اشتباه متوجه شده اید،چنین قصدی نداشتم،در مباحث نظـامی و دفـاعی هم به انـدازه خـودم،اطلاعـات دارم؛جمله ای عرض میکنم و امیـدوارم به غرض ورزی متهم نشوم،در اینکه سیاسـت مـا،هجومی نیست و دفـاعی است،شـکی نیست،امـا آیـا موشک دوربرد زمین به زمین،برای دفاع اسـتفاده میشود یا سامانه های ضـد موشکی؟...در سال از چند موشک جدید رونمایی میشود؟و در سال از چند سامانه ضد موشکی و ضد هوایی؟

البته بنده به سیاست های موشکی نقدی ندارم ؛در خصوص این قسـمت از انتقادتون در مقاله بعدی ان شاالله توضیح کاملتری خواهم داد.

فرمودید:ببخشـین یه سوآل ازتون دارم شـما مهارت هکر های متجاوز رو با چه سنگ محکی سنجیدی که گفتین با این مهارت اندک به سازمانهای ما حمله می کننـد مگر شـما از تجهیزات نصب شـده در این سازمان آمار اطلاع دارید که از چه نوع فایروالهایی به طور مثال اسـتفاده می کنند .یا با خود این هکر ها صـحبت کردید و فهمیدید غیر حرفه ای هسـتند و.... وای به هال ما اگر متخصصان حرفه ای شون مثلا حال کنند فردا صبح به ما حمله کنند چه کنیم . (خوب چرا اینقدر جو الکی میدی)

سنگ محک کشور مبدا حملات است!عربستان سعودی...

و گمان نمیکنم مقایسه بین هکرهای عربستانی و یک سرباز سازمان یافته و دولتی کشورهای توسعه یافته کار مشکلی باشد...

اما اگر گمان میکنید اقدامات کارشناسان کافی بوده،و این قوت هکر عربستانی! بوده که باعث از دسترس خارج شدن سایت ها شده،باز هم به سیاست های قبلی خود ادامه دهید،بنده هم دعا میکنم نفوذگران بعدی ضعیف تر باشند که دچار مشکل نشویم...

قسـمت بعدی نقد حضـرت عالی جای بحث بیشتر دارد،بنده هم با شـما موافقم و عرض کردم میبایست توازنی بین برقراری امنیت و حریم شخصی افراد داشته باشیم؛اما روز گذشته مقام معظم رهبری در قسمتی از صحبت هایشان به همین مطلب اشاره کردند که مبادا به بهانه مبارزه با آزادی بیان و حریم خصوصی و سایر بهانه ها جلوی دسترسی به بعضی چیزها گرفته نشود... .

کلام آخر

در ابتدا،از حضرت عالی و تمام عزیزانی که این مقاله رو مورد نقد خودشون قرار دادند،جدا سپاسگذارم.

جناب آقای رستمی

بهتر بود انتقادتان را با قلم رسمی تری مینوشتید و از الفاظ سخیف استفاده نمیکردید؛

عقـل حکـم میکنـد کـه هرکس دهـان خـود را بـه انتقـاد گشـود او دشـمن نپنـداریم،اینکـه بنـده را منـاسب برای بی بی سـی میدانیـد،ناجوانمردانه است،بنـده اگر قصد غرض ورزی و خصومت با مردم و کشورم را داشـتم،اینچنین نمینوشـتم و اگر خائن بودم از شرایط فعلی تعریف میکردم و مدعی میشدم امنیت بسیار بسیار خوبی داریم...

باز هم از حضرت عالی سپاسگذارم،خواننده نقدهای بعدی شما در ایمیلم هستم

حسین عابدین زاده

سلام

دوست عزیز اقای رستمی

با عرایض شما موافق و مخالفم که جای بحثی برای انها نمی بینم .

اما در نظر داشته باشید که سایت مرکز امار و ثبت اسناد هر دو با DotNetNuke نوشته شده اند.

بد نیست در مورد سـطح امنیت و level این زبان برنامه نویسـی تحقیقی بکنیـد.فکر نمی کنم که پلت فرم اماده ای مثل DotNetNuke مناسب سازمانهای مذکور باشن.

لینک زیر هم اسیب پذیر بودن این پلت فرم رو نسبت به حملات xss مشخص می کنه.

CVE Details

مطلب اصلی