



禪

ترکیب کلاندادهها و یادگیری ماشینی

شش استراتژی امنیتی پیادهسازی یک سازوکار دفاعی مناسب

BIG
DATA

سال گذشته میلادی، طیف گستردهای از حملات هکری با موفقیت به وقوع پیوستند . حملاتی که عمدتاً بزرگ و تأثیرگذار بودند . از حمله گسترده به زیرساختهای شرکت داین گرفته تا گزارشهایی که یاهو در ارتباط با نفوذ به سرورهای این شرکت منتشر کرده بود . هریک از این گزارشها به تنهایی طیف گستردهای از کاربران سراسر جهان را تحتالشعاع خود قرار داده بودند . در سالی که گذشت اخبار متعددی نیز در ارتباط با راهکارهای امنیتی و دستاوردهایی که شرکتهای فعال در حوزه امنیت موفق به کسب آنها شده بودند، منتشر شد که البته آن چنان که باید و شاید باعث دلگرمی کاربران نشدند .

اما حملات سال گذشته میلادی نکات ویژهای در ارتباط با حملات هکری به ما آموخت . درسهایی که بر مبنای آنها میتوانیم شش راه حل امنیت سایبری را تدوین کنیم . اگر به دنبال آن هستید تا خود را از گزند مهاجمان در امان نگه دارید، بهتر است در ابتدا فهرستی از راهکارهای امنیتی مورد نیاز خود آماده و در ادامه بر مبنای آنها استراتژیهای امنیت سازمانی را مدون کنید . ما در این مقاله شش مورد از راه حلهایی که در این زمینه به شما کمک خواهند کرد را مورد بررسی قرار دادهایم .

مطلب پیشنهادی

Brain-controlled Robots

عصر جدیدی در طراحی روباتهای هوشمند

روباتها دستورات را از ذهن انسانها میخوانند و اجرا میکنند

شاید بارها از خود این سؤال را پرسیده باشید که سازمانهایی که تحت تأثیر حملات هکری قرار میگیرند چگونه میتوانند منبع این حملات را شناسایی کنند و حتی جزییترین اطلاعات را به دست آورند . بعضی از مردم تصور میکنند به دست آوردن این جزییات یک فرآیند فوق حرفهای بوده که کمتر کاربری ممکن است قادر به تشریح آنها باشد . اما واقعیت این است که خبرهترین کارشناسان امنیتی نیز همانند شما از دل سامانههای کامپیوتری تحلیلهای خود را به دست میآورند . این تحلیلها از منابعی استخراج میشوند که ما به آنها کلاندادهها میگوییم . شاید تا به امروز عدهای بر این باور بودند که کلانهادادهها تنها در ارتباط با مسائل تجاری و آماری مورد استفاده قرار میگیرند، اما واقعیت این است که امروزه کلاندادهها در حوزه امنیت بهشدت پرکاربرد هستند . تنها اشکالی که این کلاندادهها دارند این است که درست بعد از یک نفوذ هکری میتوانند مورد استفاده قرار گیرند . به عبارت دیگر، یک نفوذ هکری سرآغازی بر جمعآوری کلاندادهها است .

1- به دنبال راهکاری فراتر از گذرواژهها باشید

تا به امروز مطالب بسیار زیادی در ارتباط با مشکلات و مصائب گذرواژهها منتشر شده است، اما با توجه به اینکه گذرواژهها هنوز هم به شکل بسیار گستردهای مورد استفاده قرار میگیرند و همواره راه حلهای مختلفی برای حل مشکل آنها ارائه شده است، پرداختن به این مفهوم هنوز هم حائز اهمیت است . پیشنهاد ما این است که مکانیسم شناسایی و احراز هویت کاربران از طریق ترکیب گذرواژه و نام کاربری را فراموش کنید . مشکلات مربوط به این ترکیب روز به روز بیشتر میشوند . بهکارگیری گذرواژهها و نامهای کاربری با استناد به سهِ دلیل زیر خطرناک هستند .

اول آنکه کاربران عمدتاً علاقهمند هستند از نام کاربری و گذرواژه یکسانی برای همه حسابهای کاربری خود استفاده کنند . همین موضوع انگیزه لازم را در اختیار مجرمان سایبری قرار میدهد تا به دنبال دستیابی به این اطلاعات باشند . زمانی که این ترکیب کشف شود دسترسی به تمام حسابها و اطلاعات امکانپذیر میشود .

دوم آنکه تعداد حملات سایبری موفقی که در یک سال گذشته به وقوع پیوستهاند زیاد بودهاند . از اطلاعات به سرقته رفته از لینکدین و یاهو گرفته تا میانافزارهای مخربی که روی روترها نصب شدهاند، در تمام موارد، هکرها به اطلاعات حساس دسترسی پیدا کردهاند . در نتیجه این توانایی را دارند تا خود را همانند کاربر اصلی به یک سیستم معرفی کرده یا از این اطلاعات برای پیادهسازی حملات فیشینگ استفاده کنند .

سومین و البته مهمترین دلیل به پیشرفتهای فناوری باز میگردد . امروزه حتی کامپیوترهای شخصی مورد استفاده از سوی کاربران نیز به سختافزارهای قدرتمندی تجهیز شدهاند . کامپیوترهایی که به پردازندههای گرافیکی قدرتمندی مجهز هستند و بهراحتی در خدمت یادگیری ماشینی و هوش مصنوعی قرار گرفته و قادر هستند با اتکا بر لغتنامهها و دیگر راهکارهای کشف و خطا، گذرواژهها را در مدت زمان کوتاهی شناسایی کنند .

اما برای حل مشکل گذرواژهها، کارشناسان امنیتی مکانیسمهای احراز هویت مختلفی را پیشنهاد کردهاند که در حال حاضر احراز هویت چند عاملی و روشهای بیومتریک که در بسیاری از اکوسیستمهای دیجیتالی مورد استفاده قرار میگیرند از جمله گزینههای پیش رو هستند .

2- اطمینان حاصل کنید، گروههای امنیتی و مدیریتی به شکل درستی یکدیگر را درک میکنند

برای آنکه مطمئن شوید این دو گروه در تعامل خوبی با یکدیگر قرار دارند، ابتدا باید شرایط فعلی شرکت یا سازمان خود را مورد بررسی قرار دهید . زمانی که مدیرعامل یک سازمان از توسعهدهندگان و متخصصان شبکهای که در آن واحد مشغول به کار هستند درخواست میکند تا گزارشی از وضعیت امنیتی ارائه کنند، کارشناسان عمدتاً سعی میکنند مزایای شرایط فعلی را برشمرده و به آسیبپذیریهای بالقوهای که امنیت سازمان را در معرض خطر قرار میدهند، کمتر اشاره کنند . در مقابل زمانی که کارشناسان امنیتی، جلساتی را با مدیرعامل ترتیب میدهند و در ارتباط با چالشهای امنیتی توضیحاتی را برای او ارائه

[illegible]

[illegible]

[illegible]

[illegible]

3- [illegible] CSIRT [illegible]

[illegible] CSIRT (Computer Emergency Response Team [illegible]) [illegible]

[illegible] CSIRT [illegible]

[illegible] CERT-FI [illegible]

[illegible] (CERT) [illegible] CSIRT [illegible]

[illegible] CSIR T [illegible]

الگوریتمهای رمزنگاری قدرتمندی در ارتباط با شبکهها استفاده و حتی نسخههای بومی از نرمافزارها را آماده کنند .»

4- در گروههایی که اطلاعات امنیتی را به اشتراک میدهند، عضو شوید

ممکن است به عنوان یک کارشناس امنیتی یا یک مدیرعامل شناختی خوبی از تهدیدات امنیتی داشته باشید، اما واقعیت این است که در طول چند سال اخیر حملات سایبری رشد افسارگسیختهای داشتهاند . استراتژیها و ابزارهای مورد استفاده هکرها دائم در حال تغییر بوده و همین موضوع باعث شده است تا نه تنها امکان نگهداری اطلاعاتی در ارتباط با تهدیدات غیر ممکن شود، بلکه فرصت بسیار کمی برای تحلیل این دادهها در اختیار شما قرار داشته باشد . در چنین شرایطی بهترین رویکردی که در اختیار شما قرار دارد این است که فرآیند شناسایی تهدیدات را خودکارسازی کنید . در این حالت، پیدا کردن راه حل برای برطرف کردن مشکل بهسادگی امکانپذیر خواهد بود . اما برای آنکه بتوانید این فرآیند را خودکارسازی کنید، ابتدا باید عضور انجمنهای امنیتی شوید؛ انجمنهایی که اطلاعات و تحلیلهای خود را با یکدیگر به اشتراک قرار میدهند . همچنین، حضور در کنسرسیومهایی که در ارتباط با تهدیدات امنیتی برگزار میشوند، بهویژه آنها که از سوی سازمانهای صنعتی برگزار میشود، در این راه به شما کمک میکنند . همواره سعی کنید با دپارتمانهای امنیتی شرکتهای شریک خود جلسات مشترکی را برقرار کنید و تحلیلهای امنیتی یکدیگر را مورد بررسی قرار دهید .

5- کلانهادادهها قدرتمندند، اما با محدودیت روبهرو هستند

امروزه کلاندادهها در هر مکانی در دسترس شما قرار دارند . مهم نیست یک شرکت داخلی یا شرکت بزرگ برونمرزی باشید . امروزه یک ارائهدهنده خدمات اینترنتی یا ارتباطی به طور معمول حجم گستردهای از دادهها را در اختیار دارد . دادههایی که از سوی مشتریان این شرکتها تولید میشوند . شرکتها به شرطی که زیرساختهای مناسبی را تدارک دیده باشند بهخوبی قادر هستند از این اطلاعات برای خدمترسانی بهتر به مشتریان خود استفاده کنند . اما کلاندادهها کاربرد دیگری نیز دارند . این دادهها به شکل عجیبی در دنیای امنیت میتوانند مورد استفاده قرار گیرند و به شرکتها در شناسایی تهدیدات کمک کنند . اما بهکارگیری آنها با یک سری محدودیتها روبهرو است ! کارشناسان امنیتی زمانی که درباره کلاندادهها صحبت میکنیم کاملاً هیجانزده و البته کنجکاو میشوند، به دلیل اینکه میدانند زمانی که نفوذی صورت میگیرد، کلاندادهها میتوانند اطلاعات زیادی در اختیار آنها قرار دهند .

بسیاری از کشورها و جوامع بینالمللی برای امنتر کردن شبکههای کامپیوتری و حتی اینترنت دست به یک همکاری گسترده زدهاند . این همکاریها به طور کلی زمینهساز شکلگیری تیم واکنشهای اضطراری رایانهای *(CERT)* یا تیم پاسخگویی به حوادث کامپیوتری *CSIRT* شده است

اما همان گونه که در پاراگراف قبل به آن اشاره کردیم، کلاندادهها با یک محدودیت روبهرو هستند . (البته بهجز یک استثنا که در انتهای مقاله به آن اشاره میکنیم .) سانتوش واراگیزا معاون شرکت Cognetyx در این ارتباط میگوید : «اگر سازمان شما هک شده است و اطلاعات مشتریان شما به سرقت رفته یا آلوده شدهاند، شما میتوانید کلاندادههایی که روی سامانهها قرار دارند را جمعآوری کنید و در ادامه این کلاندادهها را در اختیار تحلیلگران امنیتی قرار دهید . این رویکرد به شما کمک میکند دقیقاً بدانید چه اتفاقی رخ داده است و همچنین بینش شما در ارتباط با تهدیدات امنیتی را وسیعتر میکند . تحلیل کلاندادهها به شما کمک میکند مانع بروز حملات بعدی شوید . اما متأسفانه کلاندادهها زمانی مورد استفاده قرار میگیرند که یک فعالیت مجرمانه صورت گرفته باشد و در حالت عادی نمیتوانند مانع بروز یک اتفاق ناگوار شوند . این اتفاق ناخوشایند بدون شک عصبایت مشتریان را به همراه خواهد داشت تا جایی که ممکن است از سازمان شما به واسطه سهلانگاری شکایت کنند. در حالت کلی، کلاندادهها به شما این توانایی را نمیدهند تا حملات سایبری را شناسایی کنید یا مانع وقوع آنها شوید . البته زمانی که هکی انجام میشود، شما این شانس را دارید تا مانع بروز حملات مجدد شوید، اما به این نکته توجه کنید که حملات سایبری بهسادگی رخ نمیدهند . دامنه تهدیدات سایبری فراتر از حد تصور است و هرروزه رخنههای جدیدی در سامانهها شناسایی میشوند .

نکته دیگر در ارتباط با هکرها است . هکرها افراد با زکاوتی هستند که بهراحتی خود را با محیط وفق میدهند . آنها همواره رویکردهای خود را در ارتباط با حملات تغییر میدهند و به طور مداوم در حال

نویسنده :
حمیدرضا_تائبی
دسته بندی:
امنیت
تاریخ انتشار :
10:35 - 14/01/1396
برچسب:
یادگیری ماشینی - کلان داده - استراتژی امنیتی - داده های پزرگ

نشانی
□□□□:https://www.shabakeh-mag.com/security/7118/%D8%B4%D8%B4-%D8%A7%D8%B3%D8%AA%D8%B1%D8%A7%D8%AA%DA%98%DB%8C-%D8%A7%D9%85%D9%86%DB%8C%D8%AA%DB%8C-%D9%BE%DB%8C%D8%A7%D8%AF%D9%87%E2%80%8C%D8%B3%D8%A7%D8%B2%DB%8C-%DB%8C%DA%A9-%D8%B3%D8%A7%D8%B2%D9%88%DA%A9%D8%A7%D8%B1-%D8%AF%D9%81%D8%A7%D8%B9%DB%8C-%D9%85%D9%86%D8%A7%D8%B3%D8%A8