قوانین نه گانه و انکارناپذیر ریسک اطلاعات

استاد : دکتر پورابراهیمی

ترجمه: علی ثاقب موفق
خرداد ۱۳۹۹

توصیه های شرکت اینتل

قوانین نه گانه و انکارناپذیر ریسک اطلاعات

Malcolm Harkins:

- معاون گروه فناوری اطلاعات، رئیس امنیت اطلاعات (CSIO)، مدیرعامل امنیت و ریسک اطلاعات در حوزه های مالی، تدارکات و عملیات و البته دارای تجربه در فناوری اطلاعات.
- جایزه تعالی (excellence) امنیت در کنفرانس RSA سال ۲۰۱۰
- انتخاب شده بعنوان ۱۰۰ راهبر برتر حوزه فناوری اطلاعات در مجله Computerworld
- جایزه راهبری امنیت اطلاعات از (ISC)2 در سال ۲۰۱۲
- لیسانس اقتصاد و فوق لیسانس(MBA) مالی از دانشگاه کالیفرنیای آمریکا

قوانین نه گانه و انکارناپذیر ریسک اطلاعات

Malcolm Harkins:

طی سالیان، درس هایی را فرا گرفتم که به نظر می رسد علیرغم تغییرات مداوم محیطی، باقی خواهد ماند.اینها قوانین نه گانه ریسک اطلاعات نامیده می شوند

سازش، اجتناب ناپذیر است

هیچ دفاعی نمی تواند به طور کامل موثر باشد

سازمان ها بایستی درک کنند که سازش اجتناب ناپذیر است. سازش در موارد:

- **امنیت و حریم خصوصی**
- **هزینه کنترل، نگهداری و توسعه**
- **بهره وری و تجربه کاربر(کنترل ها مانعی برای سرعت کار کاربران هستند)**
- **اهداف بازار و سهم آن**
- **نیاز مشتری(امنیت و نتیجه نهایی)**

قانون اول

اطلاعات دوست دارند که رها و آزاد شوند.

مردم تمایل دارند که دائم صحبت کنند، پست کنند و اطلاعاتشان را به اشتراک بگذارند و البته آنها با انجام چنین کارهایی ریسک را بالا می برند. برای مثال:

- **صحبت در تاکسی، راهرو اداره، آبدارخانه و ... راجع به مسائل کاری**
- **رد و بدل کردن دائم اطلاعات، مطالب، تصویر، ویدئو ... در گروه ها و کانال های شبکه اجتماعی**
- **ارائه اطلاعات پروژه ها، طرح ها و برنامه های جاری و آتی محل کار در قالب پروفایل حرفه ای و شخصی و بروز رسانی دائم آنها در شبکه های اجتماعی و کسب و کار**
- **ارسال فلش مموری و سی دی حاوی اطلاعات انبوه یا ویدئوی حجیم که امکان ارسال آن توسط شبکه نیست و بدون کنترل های امنیتی**
- **ضرب المثل «زبان سرخ سر سبز می دهد بر باد» حکایت از همین دارد.**

قانون دوم

کدها و برنامه های نرم افزاری دوست دارند که غلط باشند.

نرم افزار بدون خطا نداریم. (حتی ویندوز مایکروسافت)

هر چه از یک نرم افزار کارا و کاربردی یا وب سایت بیشتر استفاده شود و کاربر بیشتری داشته باشد، بیشتر مورد توجه هکرها و ویروس ها قرار می گیرد. مثل:

- اپلیکیشن های موبایلی بانکی، وب سایت های ثبت نام خودرو، سامانه های پرداخت الکترونیک (نفوذ، جعلی)

قانون سوم

سرویس ها می خواهند که همواره On باشند.

روی هر کامپیوتر، برخی از فرایندهای پشت زمینه لازم است در حال اجراء باشند و اینها می توانند توسط هکرها کشف شوند. حتی می تواند مربوط به نرم افزارامنیتی باشد که روزانه استفاده می شود مثل بروز نگهداری سیستم با وصله های نرم افزاری یا مونیتورینگ بدافزار مثل:

- اگر سرویس های سیستم های در اختیار را بررسی کنیم، متوجه می شویم که بسیاری از سرویس های در حال اجراء بر روی موبایل یا کامپیوتر نا خواسته و یا سهوا فعال شده اند.

قانون چهارم

کاربران دوست دارندکلیک کنند.

انسانها به طور طبیعی متمایل به کلیک کردن روی لینک ها، دکمه ها و پرامت ها هستند.

بدافزارسازها به این نکته واقف هستند و از آن استفاده می کنند. در حقیقت کل صنعت فیشینگ بر اساس فرض بر این است که کاربران روی ایمیل ها و وب سایت و Pop up های فریبنده کلیک خواهند کرد که باعث بارگزاری کد مخرب بر روی سیستم آنها خواهد شد. مثل:

- کلیک بر روی لینک و یا ایمیلی که متن یا عکس فریبنده مربوط به برنده شدن در قرعه کشی، خبری جعلی و مهیج راجع به یک هنرمند و یا استخدام است.

قانون پنجم

نرم افزارهای آنتی ویروس جعلی، باعث انتشار ویروس و بدافزار شده و در حال رشد هستند.

حتی یک ویژگی امنیتی می تواند برای صدمه زدن استفاده گردد. دقیقا مثل سایر نرم افزارها، ابزارهای امنیتی توسط هکرها کشف می شوند به این معنی که قوانین ۲و۳و۴ برای قابلیت های امنیتی نیز صادق است.

مثال:

- استفاده از نرم افزارها و آنتی ویروس های رایگان و یا قفل شکسته عمومی، عاملی برای انتشار ویروس هستند.

قانون ششم

اثر یک کنترل در طول زمان بدتر می شود.

- کنترل های امنیتی تمایل دارند که ایستا باقی بمانند.اما محیطی که آنها در آن کار می کنند پویا است. به طور مثال:
- سازمانها تمایل دارند که یک کنترل و یا سیاستی را تنظیم و سپس آن را رها و یا فراموش کنند (set and forget) به طور مثال کنترل امنیتی نصب و اجراء می شود، سپس بروز رسانی آن مغفول می ماند.
- لیست rule های فایروال ماهانه بروز رسانی نمی شود.
- پسورد پیش فرض روترها و سوئیچ ها پس از استقرار تغییر نمی یابد. عدم توجه به پیام های مربوط به تاریخ اتمام بروز رسانی آنتی ویروس و فایروال نصب شده بر روی سیستم ها

قانون هفتم

کدها و نرم افزارها، نیاز دارند که اجراء شوند.

همه نرم افزارها، چه خوب و چه بد نیاز دارند که به منظور انجام کارکرد موردنظرشان، اجراء شوند.

بدافزارها به قصد خرابی ایجاد شده اند، اما تا اجراء نشوند، خفته بوده و ضرر نخواهند داشت. مثل:

- فایلهای متصل به ایمیل های فریبنده
- لینک هایی که تمنیات نفسانی کاربر را تحریک می کنند.
- برنامه های کاربردی جذاب و هیجان انگیز که کاربر را ترغیب به اجراء آنها می کنند.

قانون هشتم

کنترل ها، اصطکاک ایجاد می کنند.

کنترل های امنیتی با اثرگذاری روی کارکرد سیستم ها و فرآیندهای کسب و کار و با اجبار کاربر به طی فرایندهای سنگین، آنرا کند و آهسته می نمایند.

لذا همواره کنترل های امنیتی با فعالیت کاربری و اپراتوری کاربران دارای اصطکاک هستند. مثل:

- کنترل گیت های فرودگاه، روال تعیین هویت و اعتبار سنجی برای ورود به یک سامانه و تایپ حروف کپچا، استفاده از پسوردهای پیچیده (حروف بزرگ، کوچک، رقم و کرکتر) و سئوالهای متعاقب آن در صورت خطای پسورد، همگی منجر به خستگی کاربر می شود.
- نرم افزارهای کنترلی که پس از بالا آمدن سیستم عامل، زمانی را به خود اختصاص می دهد تا فعال، مقیم شوند و یا اینکه برای بروز رسانی از کاربر استعلام می کنند.
- پیام های مداوم نرم افزارهای کنترلی از کشف یک فایل مشکوک و درخواست از کاربر برای حذف و یا چشم پوشی از آن و پیام های اطلاع رسانی متنوع.

قانون نهم

همانطور که فرصت های دیجیتالی رشد می کند، تعهد ما برای انجام کارهای درست نیز افزایش می یابد.

همانگونه که فناوری به زندگی ما وارد می شود آسیب پذیری های آن نیز به زندگی ما ورود پیدا می کند و زندگی اجتماعی ما را متاثر از خود می سازد.

مهم است که ارزش های اخلاقی را در طراحی، توسعه و پیاده سازی این فناوری ها بکار گیریم.

امنیت و حریم خصوصی بعنوان یک مسئولیت های اجتماعی مشترک درنظر گرفته شود. مثل:

- مراقبت و به خاطر سپاری رمزهای عبور کارت های بانکی، کامپیوتر، موبایل، نرم افزرهای خاص موبایلی، شبکه های اجتماعی و تخصصی مجازی، کلاس های مجازی، سامانه های مرتبط محل کار مثل اتوماسیون اداری و ...
- حجوم اطلاعات انبوه و پراکنده از رسانه های مختلف در حوزه تخصصی و لزوم اعتبار سنجی آنها
- آگاهی از آسیب پذیری های متنوع فناوری های دیجیتالی نوظهور و تهدیدات مترتب به آن

قانون دهم

اهمیتی که تدوین کنندگان به تهیه بخشنامه، مصوبه، دستورالعمل های امنیتی و مفاد صورتجلسات امنیت اطلاعات می دهند کمتر از اهمیتی است که به اجراء و پیگیری آن می دهند.

صورتجلسات امنیت شبکه با دقت و حوصله تدوین می شود ولی برای پیگیری، اجراء،زمان بندی و مسئول آن تصمیمی گرفته نمی شود.

به طور مثال: مردم دوست دارند که بقیه، کنترل های امنیتی را رعایت کنند نه خودشان.

- رعایت کنترل های امنیتی فقط زمانی خوب است که خود فرد مشمول آن نشود.
- تدوین کنندگان ملاحظات امنیت اطلاعات و شبکه، خود تمایلی به اجرای آن ندارند.
- کاربران دوست دارند که به طور انحصاری مجوزی برای عدم اجرای دستورالعمل امنیتی داشته باشند.
- تبصره، موارد استثناء، خارج از شمول و عدم مصداق در بخشنامه ها و دستورالعمل های امنیتی برای اجراء حداقلی آن برای هر کاربر کافی است.

قوانین نه گانه انکارناپذیر ریسک اطلاعات

با تشکر

بازگشت