禪

خطمشیهای امنیتی ویژه کارمندان سازمانها

چرا کارکنان، ضعیفترین حلقه محافظت از دادههای تجاری هستند؟

زمانیکه صحبت از حفظ اطلاعات به میان میآید، نصب قدرتمندترین بستههای امنیتی تنها بخشی از تمهیداتی است که باید به آن توجه داشت. بهکارگیری قدرتمندترین بستههای امنیتی زمانی سودبخش است که سطح دانش و آگاهی کارمندان در ارتباط با مخاطرات امنیتی در حد قابل قبولی قرار داشته باشد. اگر خطمشیها و خطوط قرمز را برای کارمندان ترسیم نکرده باشید، کارمندان ناخواسته ممکن است اطلاعات حساس سازمانتان را منتشر کرده یا برای رقبا ارسال کنند. اما آموزش امنیت سایبری چیست و چه نکاتی باید به کارمندان آموزش داده شود؟ اگر به فکر بزرگتر کردن کسبوکار خود یا راهاندازی کسبوکار جدیدی هستید یا احساس میکنید کارمندان سازمان شما باید آموزشهای ویژه امنیتی دریافت کنند، این مقاله را مطالعه کنید.

ارزش دادههای سازمان شما ورای تصورتان است

تاکنون به این موضوع فکر کردهاید که اطلاعات در ظاهر بیاهمیت شرکت شما ممکن است برای شرکتهای دیگر حائز اهمیت باشد؟ اگر برای چند روز به اطلاعات شرکت خود دسترسی نداشته باشید، کسبوکار شما با چه چالشهایی روبهرو خواهد شد؟ اگر جزییات قراردادها یا سوابق مالی محرمانه شرکت در اینترنت منتشر شوند، چه تاثیرات منفی روی کسبوکارتان خواهد گذاشت؟ آیا تاکنون به این موضوع فکر کردهاید که یک کلیک شتابزده روی پیوند یا فایل دریافتی ضمیمه ایمیلی، بدون بررسی این موضوع که ایمیل از سوی چه فردی ارسالشده ممکن است چه پیامدهایی برای کسبوکارتان داشته باشد؟ پژوهش انجام شده سایت pwc در سال گذشته میلادی نشان داد، بیش از 90 درصد از شرکتهای بزرگ بهواسطه فاش شدن اطلاعات تجاری با مشکل جدی روبهرو شدهاند. بهویژه اطلاعات فنی که جزییات زیرساختها و شبکههای ارتباطی یک

lookout .

.

.

.

راهنمای گواهینامهها و دورههای آموزشی امنیت سایبری

2. هیچگاه روی پیوندهایی که نمیدانید شما را به چه سایتی هدایت خواهند کرد، کلیک نکنید

15 تا 20 درصد از نشستهای (Session) وبی که درون مرورگرها باز میشود، به دلیل کلیک کردن روی ایمیلهای ناشناس انجام میشود . بهاندازه یکچشم برهم زدن زمان میبرد که سامانهای تحت تاثیر یک حمله بدافزاری یا باجافزاری یا حتی حمله فیشینگ قرار گیرد . (بله درست خواندهاید، یک اسکریپت مخرب چند کیلوبایتی در کسری از ثانیه به درون یک سامانه وارد شده و در ادامه به دانلود بدافزارها اقدام میکند .)

قانون اول : اگر اطلاع ندارید یک پیوند شما را به چه مکانی هدایت خواهد کرد، بهتر است روی آن پیوند کلیک نکنید . قبل از کلیک کردن روی یک پیوند اگر ظاهر پیوند درست بود و شما را به دامنه درست ارجاع میدهد؛ اما در مقابل، نگارش نام دامنه فرق دارد، ممکن است به سمت یک سایت مخرب هدایت شوید. یک چنین پیوندهایی با هدف آلودهسازی یک سامانه به بدافزار یا باجافزار طراحی شدهاند .

چه تمهیداتی برای اجتناب از شکلگیری چنین حملهای باید انجام شود؟ کارمندان باید چه کاری انجام دهند؟

اگر پیوندهای دریافتی خلاصهشده و کوتاه هستند، از سایتهای زیر برای بررسی وضعیت یک پیوند استفاده کنید تا مشاهده کنید قرار است به چه سایتی وارد شوید . این تکنیک به شما کمک میکند از دام بدافزارها و هکرها به دور باشید .

http://www.checkshorturl.com/
http://www.internetofficer.com/seo-tool/redirect-check/
/http://www.shrinktheweb.com

3. هیچگاه روی ضمیمه ایمیلهایی که درخواستی برای دریافت آنها ارسال نکردهاید، کلیک نکنید

در اغلب موارد ضمیمههای ایمیل از سوی هکرها برای کنترل کامپیوتر کاربر و آلودهسازی کامپیوتر به بدافزارها استفاده میشوند . این تکنیک عمدتا در ارتباط با حملههای هرزنامهای استفادهشده، اما در شبکههای اجتماعی بهوفور استفاده میشود . اگر کارمندانتان عضو شبکههای اجتماعی هستند به آنها آموزشهای کافی را بدهید . (شکل 1)

MALICIOUS EMAIL ATTACHMENTS
Trojan-Spy.HTML.Fraud.gen
2.25%
Trojan-Downloader.HTML.Agent.aax
1.68%
Trojan.Win32.Fsysna.brtr
1.00%
Trojan-Banker.Win32.ChePro.ink
0.37%
Trojan-PSW.Win32.Fareit.auqm
0.77%
Trojan.VBS.Agent.vh
0.69%
Trojan-Downloader.Win32.Upatre.Vxd
0.68%
Trojan-Downloader.Win32.Upatre.vwi
0.65%
Trojan-Downloader.HTML.Meta.as
0.50%
Exploit.MSWord.CVE-2014-1761.k
0.49%
0%
1%
2%
3%
Top 10 malicious programs sent by email, Q2 2015

شکل 1. 10

برنامه مخرب برتری که از طریق ایمیل در نیمه دوم سال 2015 میلادی ارسال شدند .

چه تمهیداتی برای اجتناب از شکلگیری چنین حملهای باید انجام شود؟ کارمندان باید چه کاری انجام دهند؟

به فایلهای دریافتیشان مشکوک باشید (از نرمافزارهای نظارت بر فعالیت شبکه بهمنظور پیگیری فعالیتهای کاربران استفاده کنید). ما درباره فایلهایی صحبت میکنیم که نه تنها از سوی افراد ناشناس ممکن است دریافت شوند، بلکه ممکن است بدون وجود درخواست برای کارمند دیگری ارسال کرده باشند . حتی فایلهای بهظاهر عاری از مشکل همچون فایلهای آفیس مایکروسافت ممکن است به بدافزارها و آسیبپذیریهایی آلوده باشند . یکی از بهترین تمهیدات در این زمینه، غیرفعال کردن ماکروها است . ماکروها میتوانند حاوی ماژولهای مخربی باشند که به زبان ویژوال بیسیک نوشته شده و برای آلوده کردن سامانهها درون اسناد آفیس قرار میگیرند .

4. هیچگاه از شبکههای تورنت یا سایتهایی که محتویات قانونی را به شکل رایگان ارائه نمیکنند، استفاده نکنید

فایلهایی که روی شبکههای تورنت توزیع میشوند، در 90 درصد موارد دزدی هستند. در بیشتر سایتهای تورنت طیف گسترده و متنوعی از بدافزارها و ویروسها را مشاهده میکنید . درست است که این سایتها اجازه دانلود غیرقانونی فیلمها و آهنگها را میدهند، اما در مقابل سامانههای کامپیوتری را در معرض یک تهدید جدی قرار داده و راه را برای افشای اطلاعات هموار میکنند . در بیشتر کشورها سایتهای تورنت جزو سایتهای غیرقانونی هستند و فعالیت در آنها جرم بهشمار میآید . درحالیکه بیشتر مدیران تصور میکنند کارمندانشان بهاندازه آنها در مورد مشکلات امنیتی مطلع هستند، اما واقعیت چیز دیگری است. برخی از کارمندان حتی در مورد مباحث اولیه امنیت نیز اطلاعات کافی ندارند . برخی از مردم بر این باورند، هرگونه محتوایی که روی بستر اینترنت قرار میگیرد، فارغ از اینکه چه کیفیتی دارد،

Adblocker (2 .

.2

.

.5

3 תמונה

6. [illegible]

[illegible] lookout [illegible] 67 [illegible]

7. [illegible]

کنید، بهتر است ویژگی Auto-Run را غیرفعال کنید و پیش از استفاده از این تجهیزات از نرمافزار ضدویروس برای پویش دستگاههای همراه استفاده کنید .

8. هر زمان دستگاهی مفقود شد، کارمندان باید گزارش دهند

برخی از کارمندان به دلایل مختلف همچون ترس سعی میکنند، این قضیه را گزارش نکرده یا دیر اطلاع دهند. به آنها آموزش دهید هر چه از مدتزمان به سرقت رفتن یک دستگاه بگذرد، به همان نسبت شانس به سرقت رفتن و نفوذ به شبکه یک سازمان افزایش پیدا میکند . دسترسی غیرمجاز به اطلاعات قراردادها، مناقصهها، فرمهای مالیاتی کارمندان یا سایر اطلاعات حساس پیامدهای جدی برای یک سازمان به همراه دارد .

مطلب پیشنهادی

اطلاعاتی دست نیافتنی و غیر قابل مشاهده

8 ابزار برتر رمزگذاری اطلاعات

9. کارمندان را مجبور کنید از گذرواژههای غیرمتعارف استفاده کرده و آنها را دائم تغییر دهند

پیشرفت فناوری باعث شده، گذرواژهها در مقابل حملههای هکری کارایی کمتری داشته باشند، باوجوداین، هنوز هم یک گذرواژه قدرتمند برگ برنده یک سازمان است . به کارمندان خود آموزش دهید از گذرواژههای قدرتمندی که بیشتر از 14 کاراکتر بوده و ترکیبی از لغات بزرگ، کوچک، اعداد و نشانهها است استفاده کنند . کارمندان نباید از گذرواژهها برای بیش از یک حساب کاربری استفاده کنند . گذرواژه دسترسی به کامپیوتر سازمان باید با گذرواژهای که در منزل خود از آن استفاده میکند، متفاوت باشد . گذرواژهها نباید با سایر کارمندان به اشتراک قرار گیرد، گذرواژهها باید در بازههای زمانی کوتاهمدت تغییر کنند . برای راحتی کار به کارمندان پیشنهاد دهید، از ابزارهای مدیریت گذرواژه همچون LastPass برای مدیریت گذرواژهها استفاده کنند . احراز هویت دو مرحلهای با اضافه کردن یک لایه امنیتی مضاعف در کنار گذرواژهها مانع از آن میشود تا هکرها بتوانند مکانیزمهای امنیتی را بهراحتی دور بزنند .

سخن پایانی

برخی از افراد با اصول اولیه امنیت آشنایی کافی دارند و میدانند که حریم خصوصی چیست و هکرها همواره آماده هستند تا اطلاعات شخصی یا کاری آنها را به سرقت ببرند، با این حال بهدرستی نمیدانند از دانش خود در چه مکانی باید استفاده کنند . به کارمندان خود هشدار دهید که سهلانگاری و عدم توجه به هر یک از معیارهای امنیتی ممکن است چه عواقبی برای آنها و سازمان به همراه داشته باشد .

نویسنده :
حمیدرضا تائبی
دسته بندی:
امنیت
تاریخ انتشار :
05:50 - 17/07/1398
برچسب:
حفاظت از داده های تجاری - داده های سازمان - حفظ امنیت داده ها - حفظ حریم خصوصی - کارمند - نقش

[illegible]
https://www.shabakeh-mag.com/security/15716/%DA%86%D8%B1%D8%A7-%DA%A9%D8%A7:[illegible]
%D8%B1%DA%A9%D9%86%D8%A7%D9%86%D8%8C-
%D8%B6%D8%B9%DB%8C%D9%81%E2%80%8C%D8%AA%D8%B1%DB%8C%D9%86-
%D8%AD%D9%84%D9%82%D9%87-%D9%85%D8%AD%D8%A7%D9%81%D8%B8%D8%AA-
%D8%A7%D8%B2-%D8%AF%D8%A7%D8%AF%D9%87%E2%80%8C%D9%87%D8%A7%DB%8C-
%D8%AA%D8%AC%D8%A7%D8%B1%DB%8C-
%D9%87%D8%B3%D8%AA%D9%86%D8%AF%D8%9F