اشتباهاتی برای سقوط؛ راه‌حل‌هایی برای صعود

نکات امنیتی مهم برای کاربران سازمان‌ها

در حالی که کارشناسان امنیتی مرتباً به کاربران هشدار می‌دهند که به حداقل اصول امنیتی توجه کنند، اما باز هم شاهد سهل‌انگاری‌های کاربران هستیم. این سهل‌انگاری‌ها نه تنها آرامش کاربران را به هم می‌ریزد، بلکه در بیشتر موارد تبعات مالی فراوانی را برای آن‌ها به همراه دارد. سایت «cio» از جمله سایت‌های معتبر فضای مجازی است که همواره به بررسی موضوعات و رخدادهای روز می‌پردازد. مقاله اصلی این سایت بار دیگر به موضوع «چگونه می‌توانیم عادت‌های بد امنیتی را از خود دور کنیم؟» اختصاص پیدا کرد.

این مقاله که چهارم آوریل 2016 به قلم «شارون فلورنتاین» نگارش شده است، یک‌بار دیگر به کاربران سامانه‌های مهم و سازمان‌های بزرگ در زمینه پیاده‌سازی استراتژی‌های امنیتی کارآمد برای دوری جستن از مخاطرات امنیتی، توصیه‌هایی کرده است. بر همین اساس، ما نیز در این مقاله بر آن شدیم تا ضمن پرداختن به موضوعات ارائه‌شده در آن مقاله، نگاهی نیز به راهکارهایی بیندازیم که برای افزایش امنیت گذرواژه‌ها استفاده می‌شوند. همچنین به طور مختصر به نحوه پیاده‌سازی خط‌مشی‌های امنیت شبکه نیز خواهیم پرداخت. پیشنهاد می‌کنیم از ابتدای سال جاری به این توصیه‌ها توجه کنید تا یک سال را به دور از استرس و نگرانی درباره بدافزارها و انواع مختلف تهدیدها پشت سر نهید.

مطلب پیشنهادی

ده اشتباه مرگ‌بار در مدیریت امنیت اطلاعات

عواقب بی‌توجهی به مسائل امنیتی فراتر از حد تصور است

تشویش و بی‌قراری از جمله عادت‌های ناپسند به شمار می‌روند، اما هیچ‌یک از این رفتارها به اندازه کافی مخرب نیستند که بتوانند شرکتی را به زانو درآورند. اما زمانی که صحبت از امنیت به میان می‌آید، شاهد رفتارها و عادت‌های ناپسندی از کاربران سازمانی هستیم که می‌توانند زمینه‌ساز ورشکستگی سازمان شوند؛ به‌طوری که شرکتی را در برابر حملات هکری آسیب‌پذیر می‌کنند و در نهایت منجر به از دست رفتن داده‌ها یا سرقت آن‌ها می‌شوند. همه این اتفاقات به دلیل رخنه‌های امنیتی شبیه به یکدیگر رخ می‌دهد. اما خبر خوب این است که با توجه و دقت به اصول اولیه و ساده دنیای فناوری، آموزش کاربران در خصوص مسائل امنیتی، انتخاب بهترین مکانیزم

امنیتی و به‌کارگیری راه‌حل‌هایی که در این زمینه وجود دارد، می‌توانیم تا حدود بسیار زیادی مخاطرات امنیتی را کاهش دهیم. «جاناتان کرو»، مدیر ارشد محتوا در شرکت امنیتی «بارکلی» توصیه‌های ساده‌ای را برای بهبود وضعیت امنیتی سازمان‌ها و کاربران پیشنهاد کرده است. اگر کارمندان سازمان‌ها به این نکات توجه کرده و از آن‌ها در زمان کار با سامانه‌های مهم استفاده کنند، نه تنها سطح درک آن‌ها از اصول امنیتی بالاتر می‌رود، بلکه توانایی مقابله با تهدیدات امنیتی را نیز خواهند داشت.

خط مشی امنیت شبکه سازمانی خود را مطابق با استانداردهای جهانی آماده‌سازی کنید

برای هر کارشناس امنیتی، تلاش برای نگارش سیاست امنیتی (Security Policy) رویکرد دشواری به شمار می‌رود. به دلیل اینکه ماهیت این مفهوم، به خودی خود پیچیده است و پیاده‌سازی چنین الگویی کار چندان ساده‌ای نیست. کارشناس امنیتی ابتدا باید توانایی درک مشکلات و چالش‌های پیش رو را داشته باشد. وی همواره با پرسش‌هایی نظیر چه چیزی باید نگارش شود؟ چگونه باید نگارش شود؟ چه کسی مسئول آن خواهد بود؟ و موضوعاتی از این دست روبه‌رو خواهد بود. این‌ها از جمله سؤالات راهبردی هستند که پیش روی هر کارشناس امنیت شبکه قرار دارند. تدوین و آماده‌سازی استراتژی امنیت اطلاعات بیشتر از اینکه فن باشد، هنر است. هیچ کارشناس امنیتی را پیدا نخواهید کرد که اعلام کند در مدت‌زمان دو روز، توانایی آماده‌سازی دستورالعمل 80 صفحه‌ای را برای سازمان شما دارد. در حالی که تعدادی از نیازمندی‌های مربوط به این سیاست‌گذاری ممکن است باعث کاهش هزینه یا کم کردن دردسرهای تدارکاتی برای محیط‌های مشخصی باشد، اما فهرستی که در ادامه مشاهده خواهید کرد، شبیه به فهرستی است که مردم در زمان تعطیلات آماده کرده‌اند و هر آن چیزی را که به آن علاقه‌مند هستند، در آن قرار می‌دهند؛ به استثنای این مورد که این فهرست ویژه یک محیط امنیتی، آماده‌سازی شده است، این سیاست‌گذاری به‌گونه‌ای است که به مرور زمان و همگام با افزایش سطح تجربیات شخصی به تکامل رسیده، الگوی تهدیداتی که شبکه را به مخاطره می‌اندازند تغییر داده است و در نهایت، امنیتی سازگار با این حملات را ارائه می‌کند. مهم‌ترین اصلی که در زمان نگارش دستورالعمل امنیت شبکه لازم است به آن توجه کنیم، این است که مجال تنفسی برای الگوی سیاست‌گذاری امنیتی در نظر بگیریم تا همواره سند پویا و زنده‌ای در اختیار داشته باشیم. در حوزه امنیت همه چیز به‌سرعت در حال تغییر است، در نتیجه سیاست امنیتی همواره باید سرعت خود را با این تغییرات حفظ کند.

منابع موجود و تکامل تدریجی سیاست‌گذاری

اولین پرسش کارشناس امنیت شبکه از خود، این است که چگونه می‌تواند ایده‌ها و استراتژی‌های خود را به شکلی مدون و کاربردی به سیاست امنیتی تبدیل کند؟ اکثر کارشناسان امنیتی سریعاً به این حقیقت آگاه می‌شوند که پشتیبانی مدیران اجرایی برای اجرا و حمایت از خط مشی امنیتی، از ارکان اصلی موفقیت برنامه امنیت اطلاعات است. برای اینکه پشتیبانی به وجود بیاید و تداوم پیدا کند، کارشناس امنیت شبکه باید به دو نکته توجه کند. در گام اول، ضروری است که دامنه سیاست‌گذاری به‌درستی و روشنی تشریح شود و دوم اینکه اطلاع‌رسانی درباره دستورالعمل‌های مرتبط با سیاست‌گذاری به شیوه جامع و کارآمدی به کارکنان منتقل شود. منابع موجود به‌خوبی نشان می‌دهند که فرایند عنوان‌بندی دستور العمل مرتبط با سیاست امنیتی، دربرگیرنده مؤلفه‌هایی همچون مقصود (Purpose)، هدف (Objective)، کارکرد (Applicability)، توزیع (Distribution)، اجرا (Enforcement) و نظارت (Monitoring) است. برای مثال، در بسیاری از کشورها از استاندارد بین‌المللی ISO/IEC 27001:2005 به‌عنوان الگویی برای استقرار سیستم مدیریت امنیت اطلاعات استفاده می‌شود.

کارشناس امنیت شبکه ممکن است در نظر داشته باشد سیاست‌گذاری مدنظر خود را با هدف نشان دادن مخاطرات آماده‌سازی کند. اما این جمله به چه معنا است؟ ریسک‌های امنیت شبکه با نشان دادن استانداردهای امنیتی تعریف می‌شوند. راهنمای خط مشی امنیت شبکه NSPM ، سرنام Network Security Policy Manual، هم بر استاندارد ISF ، سرنام Information Security Forum، که متشکل از تجربیات 260 شرکت و سازمان بین‌المللی در زمینه اطلاعات و امنیت اطلاعات است تأکید دارد و هم بر ایزو 17799:2005 که از استانداردهای ارائه‌شده از سوی ISO است. سند عمومی NSP که سند بلندبالایی است بر کنترل دسترسی به داده‌ها، رفتارهای مرورگرها، نحوه به‌کارگیری گذرواژه‌ها، رمزنگاری، ضمیمه‌های ایمیلی و در کل مواردی که قوانین و ضوابطی را برای افراد و گروه‌ها ارائه می‌کند، تأکید دارد. در این سند اعلام شده است که کارشناس امنیت شبکه که مسئولیت تنظیم خط مشی امنیتی

شبکه را بر عهده دارد، باید سلسله مراتبی از مجوزهای دسترسی کاربران را آماده‌سازی کند و به هر کاربر بر اساس شرح وظایفش اجازه دسترسی به منابع مختلف را دهد. برای این منظور سازمان‌های بزرگی در هر کشور همچون مؤسسه ملی فناوری و استانداردها NIST، سرنام
National Institute of Standards and Technology، در ایالات متحده، مسئولیت تدوین استانداردها و خط مشی‌ها در امنیت اطلاعات را بر عهده دارند. روش ساده برای نوشتن دستورالعمل‌های خط مشی تبدیل زبان استاندارد به یک دستورالعمل خط مشی، با نشان دادن سطح قابل پذیرش ریسک‌پذیری سازمان است. در زمان نگارش خط مشی سازمان باید به این نکته توجه کرد که مقدمه باید هم بر خط مشی و هم هدف کنترلی خط مشی تقدم داشته باشد. برای این منظور پیشنهاد می‌کنیم نگاه دقیقی به استاندارد ISF و همچنین ایزو 17799 بیندازید.
برای مثال، نمونه‌ای از تدوین یک دستورالعمل خط مشی در خصوص عیب فنی منابع شبکه و اطمینان پیدا کردن از این موضوع که مؤلفه‌های شبکه می‌توانند به حالت اول خود بازگردند، می‌تواند همانند مثال زیر باشد:

کنترل قابلیت ارتجاعی شبکه برگرفته از ISF Network Resilience Control (NW1.3.3)

مقدمه: ریسک درست عمل نکردن تجهیزات حیاتی ارتباطی، نرم‌افزار، پیوندها و سرویس‌ها باید کاهش پیدا کند؛ به‌طوری که اطمینان حاصل شود می‌توان مؤلفه‌های کلیدی شبکه را در بازه‌های زمانی بحرانی جایگزین کرد.
دستور العمل خط مشی: به‌منظور برطرف کردن موقتی خطر و تأثیر خرابی‌ها، ضروری است برای بخش‌های حیاتی سیستم اولویت‌هایی در نظر گرفته شده و اطمینان حاصل شود که مؤلفه‌های کلیدی شبکه در بازه زمانی هدف قابلیت جایگزینی و برگشت به حالت اولیه را دارند.

به‌کارگیری گذرواژه‌های یکسان یا ساده برای حساب‌های کاربری مختلف

شرکت امنیتی مدیریت گذرواژه «SplashData» هر سال از گذرواژه‌های غیرایمن به‌عنوان یکی از عادت‌های بد کاربران اینترنتی یاد کرده و فهرستی از بدترین گذرواژه‌ها را فهرست و منتشر می‌کند. لازم به توضیح نیست که هنوز هم بسیاری از کاربران از گذرواژه‌هایی همچون 123456 یا Password به صورت کاملاً عادی استفاده می‌کنند. گذرواژه‌هایی این‌چنینی مصداق ارسال دعوت‌های جذاب برای هکرها هستند. در حالی که کاربران به‌راحتی می‌توانند گذرواژه‌های مختلف و پیچیده را برای حساب‌های کاربری خود به یاد بیاورند، مشخص نیست به چه دلیل از گذرواژه‌های ساده و بدتر از آن یکسان استفاده می‌کنند.
راه‌حل: کرو در این خصوص به کاربران پیشنهاد می‌کند: «از یکی از برنامه‌های مدیریت گذرواژه‌ها استفاده کنید. این برنامه‌ها نه تنها توانایی تولید گذرواژه‌های تصادفی و ایمن را دارند، بلکه به ویژگی رمزنگاری و یادآوری آن‌ها مجهز هستند. به همین دلیل کاربران در این زمینه با مشکل خاصی روبه‌رو نخواهند بود.»

کلیک کردن روی لینک‌ها یا ضمیمه‌ها بدون بررسی دقیق آن‌ها

این روزها هکرها استراتژی‌های خود را به طرز بسیار وحشتناکی تغییر داده‌اند؛ به‌گونه‌ای که سعی می‌کنند پیامی که برای کاربر ارسال می‌کنند، ظاهری قانونی داشته باشد. برای این منظور آن‌ها از ترفندهای مهندسی اجتماعی برای ارسال ویروس یا دسترسی به سیستم‌های خصوصی استفاده می‌کنند. پیام‌های ارسال‌شده حتی در ظاهر ممکن است از سوی منابعی ارسال شوند که کاربران آن‌ها را می‌شناسند یا به آن‌ها اعتماد دارند.
راه حل: کرو در این باره به سازمان‌ها پیشنهاد می‌کند: «به کاربران خود آموزش دهید که چگونه می‌توانند با نگهداشتن ماوس روی لینک‌ها یا ابرلینک‌ها مکانی را مشاهده کنند که سمت آن هدایت خواهند شد. اگر سایتی با لینکی هماهنگ نبود یا مشکوک به نظر می‌رسید، روی آن لینک کلیک نکنید. همچنین کاربران نباید هر ضمیمه‌ای را که برای آن‌ها ارسال می‌شود، باز کنند؛ به ویژه ضمیمه‌هایی که انتظار دریافت آن‌ها را نداشته‌اند.»

به کارگیری دستگاه‌های جدید ضامن موفقیت

بسیاری از کاربران بر این باور هستند که با خرید دستگاه‌هایی که تازه به بازار عرضه شده است، در برابر بسیاری از حملات مصون هستند و به مرور زمان است که دستگاه آن‌ها در برابر حملات هکری ضعیف می‌شود. اما این طرز

تفکر درست نیست. «الینور سایتا» مدیر بخش فنی مؤسسه «International Modern Media» در این باره می‌گوید: «ابزارها و دستگاه‌هایی که تازه به بازار عرضه می‌شوند، بیشتر همراه با برنامه‌های تبلیغاتی در اختیار کاربران قرار می‌گیرند. در بیشتر موارد این برنامه‌های تبلیغاتی آسیب‌پذیری‌های مختلفی را در خود جای داده‌اند.» نرم‌افزار سوپرفیش که همراه با لپ‌تاپ‌های لنوو در اختیار کاربران قرار گرفته بود، نمونه‌ای از این موارد بود.» نکته دیگری که درباره این دستگاه‌ها وجود دارد به در پشتی تعبیه‌شده روی آن‌ها بازمی‌گردد. درهای پشتی در بیشتر موارد به دلیل درخواست نهادهای دولتی یا استفاده شرکت‌های سازنده، روی محصولات قرار می‌گیرند. اما واقعیت این است که درهای پشتی یک آسیب‌پذیری امنیتی هستند که هر شخصی با داشتن اطلاعات فنی ممکن است به آن‌ها دسترسی داشته باشد. درهای پشتی حقیقتی هستند که هیچ‌گاه از میان نخواهند رفت و فقط به مرور زمان نحوه قرارگیری یا شناسایی آن‌ها دستخوش تغییرات می‌شوند.

راه حل: در زمان خرید ابزارهای جدید به این نکته توجه کنید که جدید بودن همیشه تضمین‌کننده امنیت نیست. اگر در نظر دارید دستگاه جدیدی به‌ویژه دستگاهی هوشمند خریداری کنید، سعی کنید در خرید آن کمی تأمل کنید تا به بازار عرضه شود و در ادامه ایرادات یا آسیب‌پذیری‌های آن شناسایی شوند.

سهل‌انگاری در نصب به‌روزرسانی‌ها یا وصله‌ها

زمانی که یک آسیب‌پذیری در نرم‌افزاری شناسایی شده و وصله مربوط به آن عرضه می‌شود، شمارش معکوسی آغاز می‌شود که در فرصت باقی‌مانده نهایت بهره‌برداری از آسیب‌پذیری انجام شود. کرو در این خصوص می‌گوید: «آمارها نشان می‌دهند که هکرها هیچ‌گاه زمان را هدر نمی‌دهند، در سال 2014 میلادی، نزدیک به نیمی از آسیب‌پذیری‌ها و سوءاستفاده‌هایی که از آن‌ها شده بود؛ به‌طور میانگین در مدت زمان دو هفته انجام گرفته بود؛ در حالی که وصله‌ها معمولاً در همان ابتدای کار عرضه می‌شوند.»

راه حل: کرو در این باره گفته است: «سعی کنید در زمینه دریافت وصله‌ها از برنامه منظم و ساختمندی استفاده کنید. این کار باعث می‌شود تا به طور خودکار به‌روزرسانی‌ها و وصله‌ها دریافت شوند. مزیت این راهکار در این است که حتی اگر به دلیل مشغله کاری فراموش کردید وصله‌ای را دریافت کنید، این کار به طور خودکار انجام می‌شود و همراه شما را در امنیت نگه می‌دارد.»

به‌کارگیری وای‌فای عمومی

هر کاربری با شنیدن این جمله که وای‌فای رایگان در اختیار او قرار دارد، وسوسه می‌شود تا از آن استفاده کند. در مکان‌هایی همچون رستوران‌ها یا فرودگاه‌ها که وای‌فای عمومی عرضه می‌شود، مردم برای انجام کارهای خود از آن استفاده می‌کنند. کرو در خصوص این موضوع گفته است: «باید به این نکته توجه کنیم که رایگان بودن و عمومی بودن همیشه به معنای در اختیار داشتن فناوری به شکل ایمن نیست. این چنین ارتباطاتی به میزان قابل توجهی خطرناک هستند.»

راه حل: کرو برای دوری از این خطر پیشنهاد می‌کند:«در چنین شرایطی بهتر است از VPN استفاده کنید. این مکانیزم ترافیک را رمزنگاری کرده و نشست‌های مرورگر شما را ایمن می‌سازد. حتی اگر شرکت، سازوکار VPN را در اختیارتان قرار نمی‌دهد، سعی کنید در خصوص فواید و مزایای چنین مکانیزم ارتباطی اطلاعات مورد نیاز را به دست آورید.»

به‌کار نگرفتن مکانیزم احراز هویت دوعاملی

«الکس استاموس» مدیر ارشد امنیت شرکت فیسبوک درباره گذرواژه‌ها گفته است: «سایت‌های خبری به طور گسترده بر مکانیزم‌های پیچیده و چندلایه حمله که هکرها استفاده می‌کنند، متمرکز شده‌اند. این شیوه اطلاع‌رسانی به کاربر این پیام را القا می‌کند که او در برابر حملات کاملاً آسیب‌پذیر بوده و هیچ راه دفاعی در اختیار ندارد. اما در بیشتر موارد این جمله درست نیست. تنها سازمان‌های دولتی آن هم در رده‌های بسیار بالا، توانایی نفوذ به هر سیستمی را دارند. اما در مقابل هکرها، حتی هکرهای سازمان‌یافته، دفاع قابل قبولی وجود دارد.»

راه حل: استاموس در این خصوص به کاربران پیشنهاد می‌کند: «مکانیزم احراز هویت دوعاملی را که اغلب با ارسال کدهایی برای تلفن‌های هوشمند کار می‌کنند، در حساب‌های کاربری و شبکه‌های اجتماعی استفاده کنند. هکرها

عمدتاً در تلاش هستند حساب‌های کاربری را که روی شبکه‌های اجتماعی قرار دارند، هک کنند و کنترل آن‌ها را به دست گیرند. به دست آوردن حساب کاربری افراد در شبکه‌های اجتماعی تنها برای آسیب رساندن به افراد هک نمی‌شوند، هکرها می‌توانند از چنین حساب‌هایی به بهترین شکل ممکن استفاده کنند و سودهای کلانی به جیب بزنند. در کنار مکانیزم احراز هویت دو عاملی، سعی کنید از ابزار مدیریت‌کننده گذرواژه‌ها برای حساب‌ها و سرویس‌های کاربری خود استفاده کنید.»

این فرض که یادآوری گذرواژه‌های طولانی کار مشکلی است

بسیاری از کاربران اعلام می‌کنند که توانایی یادآوری گذرواژه‌های طولانی را ندارند. به همین دلیل بسیاری از کاربران برای سادگی کار سعی می‌کنند از ترکیباتی همچون سال تولد و شماره شناسنامه خود برای ورود به سایت‌های مختلف استفاده کنند؛ به دلیل اینکه یادآوری گذرواژه‌های مختلف برای سایت‌های مختلف کار سختی به شمار می‌رود. همچنین بعضی از کاربران نیز تمایلی به استفاده از برنامه‌های مدیریت گذرواژه‌ها ندارند. اگر جزو این گروه از کاربران هستید، هنوز هم راهکاری برای شما در زمینه ساخت گذرواژه‌های منحصربه‌فرد وجود دارد.

راه حل: برای اینکه نیازی به یادداشت کردن گذرواژه‌های خود نداشته باشید و همچنین بتوانید به ساده‌ترین شکل ممکن گذرواژه‌های خود را به یاد آورید، می‌توانید از ترکیب نام سایت مورد بازدید در انتهای گذرواژه خود استفاده کنید. «لوییس کرنر» مدیر فنی بخش امنیتی کلاود شرکت «پاندا» در این باره گفته است: «برای ساخت گذرواژه‌ای منحصربه‌فرد و یادآوری ساده آن، نام سایت را به انتهای گذرواژه انتخابی خود اضافه کنید. برای مثال برای سایت bank.com واژه -bank را به‌عنوان پسوند گذرواژه یا در حساب‌های مورد استفاده در شبکه‌های اجتماعی از -linkedin یا -twit و مانند این‌ها به‌عنوان پسوند گذرواژه خود استفاده کنید.»

این فرض که امنیت، مشکل فناوری اطلاعات است

در بیشتر شرکت‌ها بسیاری از کاربران بر این باور هستند که همواره گروه‌های فنی و راه‌حل‌های امنیتی در محل وجود دارند تا برای حفاظت و کمک به تعاملات آنلاین وارد عمل شوند. این موضوع کاملاً صحیح است، اما هر کاربری خود مسئول آن چیزی است که انتخاب کرده و این انتخاب بر امنیت فردی و امنیت شرکتی که در آن کار می‌کند، تأثیرگذار خواهد بود. بخش عمده‌ای از نقض‌های داده‌ای و حملات سایبری از زمانی آغاز می‌شوند که کاربر روی لینکی که نباید کلیک می‌کرده، کلیک کرده، لپ‌تاپ خود را در تاکسی جا گذاشته یا آن را به شبکه وای فای عمومی متصل کرده است.

راه حل: کرو در این باره گفته است: «آموزش، یادگیری و تکرار نکات آموزشی، رمز دوری جستن از چنین مشکلاتی است. اطمینان حاصل کنید کاربران شما بهترین اقدامات امنیتی را به طور روزانه انجام می‌دهند.» یادگیری بیشتر درباره مخاطرات امنیتی، باعث کم شدن تهدیدها می‌شود و کاربران می‌توانند به‌خوبی با تکنیک‌های اولیه دفاعی در برابر پیوندهای ضعیف آشنا شوند.

منابع: ۱ + ۲ + ۳

==========

شاید به این مقالات هم علاقمند باشید:

بررسی تحلیلی علل استقرار ERP در سازمان‌ها

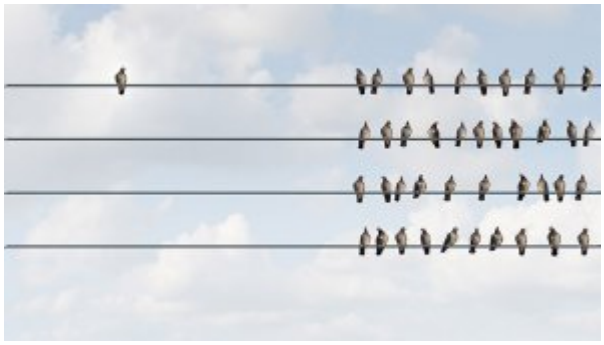
10 عاملی که پروژه‌های ERP را به شکست می‌کشاند

نگاهی به مدل کسب‌وکار شرکت آرم

10 نکته کلیدی برای موفقیت در مصاحبه دکتری

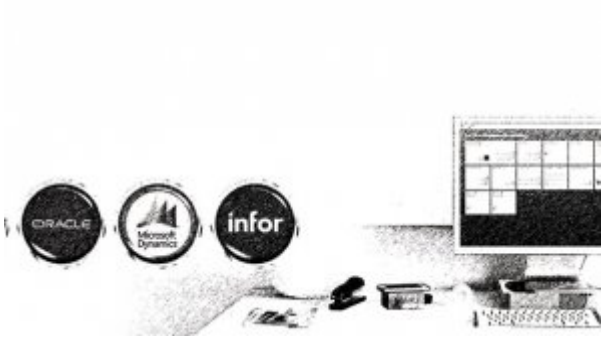
کسب و کار شرقی

6 ویژگی اصلی رهبر منابع انسانی



با این ده نشانه به طور حتم یک رهبر کسب وکار هستید

۵ اصل کلیدی موفقیت حیرت‌انگیز ایلان ماسک



چالش‌های پیاده‌سازی ERP

تاریخ انتشار:
13 خرداد 1395

نشانی منبع: https://www.shabakeh-mag.com/security/3441