BYOD، داده‌های سازمان، ابزارهای کارکنان

مدتی است که ابزارهای همراه کارکنان، در عمل به بخشی از ناوگان ارتباطی و پردازشی شرکت‌ها و سازمان‌ها تبدیل شده است. به نظر می‌رسد که چند سالی است وارد عصر (BYOD (Bring Your Own Device شده‌ایم؛ عصری که به گزارش موسسه گاردنر، نیمی از سازمان‌ها و شرکت‌ها، از BYOD به عنوان یک سیاست راهبردی در کسب‌وکار و فعالیت‌های خود استفاده می‌کنند. اما BYOD به چه معنایی است؟

بر اساس تعریفی که واژه نامه تخصصی پی سی مگزین از این واژه به دست می‌دهد، **BYOD** به وضعیتی اشاره دارد که ابزارهای ارتباطی، پردازشی و حتی ذخیره‌سازی کارکنان، مانند گوشی‌های هوشمند، تبلت‌ها، لپ‌تاپ‌ها، درایوهای یو اس بی و دیگر تجهیزات همراه، با توانایی اتصال به شبکه شرکت، برای مقاصد کسب وکار و تجاری مورد استفاده قرار می‌گیرند. بر اساس برآورد موسسه IDC در سال 2011 حدود 41 درصد سازمان های بزرگ از این روش برای پیشبرد کارهایشان استفاده می‌کردند. بدیهی است که این درصد در سال‌های اخیر به شدت افزایش یافته است. نکته مهم اما، تنها سخت‌افزارها نیستند؛ بلکه هر کدام از دستگاه‌های کارکنان حاوی ده‌ها و بلکه صدها برنامه و اپلیکیشن هستند که می‌تواند در خدمت اهداف شرکت‌ها قرار گیرند.

چرا BYOD؟

یکی از مزیت‌های **BYOD** صرفه‌جویی در هزینه‌های سخت‌افزاری است به ویژه در جایی که منابع نسبتا کمی برای این بخش وجود دارد. تصور کنید که یک سازمان که صدها و حتی هزاران کارمند دارد، مجبور باشد برای تمام کارکنانش ابزارهای ارتباطی مانند اسمارتفون، لپ‌تاپ یا تبلت و برنامه‌های مورد نیاز آن‌ها را فراهم کند؛ به ویژه اگر در نظر داشته باشید که در کشورهای توسعه‌یافته، برای بسیاری از نرم افزارها باید پول پرداخت؛ به‌طور حتم بخش قابل توجهی از منابع مالی سازمان باید به این امر اختصاص یابد.
از سوی دیگر، در دسترس بودن کارکنان در ساعات و روزهای مختلف و وجود داده‌ها و اطلاعات و برنامه‌های شرکت در دستگاه‌های متحرک آن‌ها، باعث می‌شود که مدیران شرکت در هر زمانی به آن‌ها دسترسی داشته باشند و بتوانند بخشی از کارها را پیش ببرند. در عین حال، شبکه ارتباطی گسترده‌ای میان کارکنان پدید می‌آید که می‌توانند چه در ساعات و روزهای کاری و چه غیر آن با هم در تعامل باشند. این وضعیت به ویژه برای شرکت‌هایی که به لحاظ جغرافیایی شعبه‌های متعدد دارند و یا کارشان به گونه‌ای است که تعداد زیادی از کارکنان آن ها در نقاط مختلف در تردد هستند، اهمیت خاصی پیدا می‌کند.
شرکت‌ها و موسساتی که به علاقمندی و وفاداری کارکنان اهمیت می‌دهند، می‌توانند از طریق ایجاد صفحات خاص در شبکه‌های اجتماعی و یا سایت‌های خود و ایجاد محتوای برانگیزاننده و در عین حال سرگرم‌کننده، نوعی همبستگی را در میان آن‌ها و برند خود پدید آورند.
از سوی دیگر، وجود این دستگاه‌ها نزد کارکنان شرکت که به خوبی با آن‌ها آشنا و اخت هستند، نوعی چابکی و

تحرک را به آن‌ها می‌بخشد و باعث می‌شود که در هر جایی که هستند، و در هر زمانی بتوانند بخشی از کارهای حرفه‌ای خود را انجام بدهند. دیگر انجام کار، منوط به حضور در دفتر شرکت و یا ساعات 9 تا 5 نیست. اگر نگاهی با دقت به اطراف خود داشته باشید، کسانی را خواهید دید که در ساعات و روزهای غیرکاری، مشغول انجام کارهای مربوط به شرکت خود هستند.

این وضعیت نه تنها به نفع صاحبان کسب‌وکارها است بلکه در بسیاری از موارد باعث می‌شود که کارکنان نیز با انجام کارها از این طریق، نه تنها در وقت خود صرفه‌جویی کنند، بلکه از فشارهای مربوط به رفت و آمد به محل کار و حضور در یک زمان و مکان خاص اجتناب کنند. این که آن‌ها بتوانند بخشی از کار خود را در زمانی غیر از ساعات معین کاری انجام بدهند، نه تنها باعث ایجاد نوعی استقلال و آزادی حرفه‌ای برای آن‌ها می‌شود، بلکه رضایت و کارآمدی و حتی خلاقیت بیشتری را به همراه خواهد داشت.

میزان استقبال از **BYOD** در نقاط مختلف جهان نیز متفاوت بوده است. در حالی که اروپایی‌ها به شکل محتاطانه‌تری با این استراتژی برخورد کرده‌اند، کارفرمایان آمریکایی دو برابر بیشتر از همتایان اروپایی خود از **BYOD** استقبال کرده‌اند. همچنین مطالعات حاکی از آن است که کاربران در کشورهایی مانند چین، هند و برزیل تمایل بیشتری دارند که از ابزارهای موبایل خود به عنوان ابزارهای سازمانی استفاده کنند.

چالش‌های BYOD

بدون هیچ تردیدی، امنیت، بزرگ‌ترین چاش پیش روی **BYOD** است. وقتی قرار است تعداد زیادی کاربر، هر کدام با دستگاه‌ها و برنامه‌های خود وارد شبکه سازمان شوند، بی‌شک، سیستم می‌تواند به طور کامل با خطر مواجه شود. مدیریت ناوگان متنوعی از سخت‌افزارهای همراه و برنامه‌های آن‌ها کار چندان ساده‌ای نخواهد بود. خطر تنها در این نیست که بدافزارهای مختلف از طریق دستگاه‌های کارکنان به سیستم منتقل شوند؛ بلکه در چنین شرایطی حفاظت از داده‌های شرکت که در واقع بخشی از اموال و دارایی‌ها آن به شمار می‌آید، بسیار دشوار می‌شود. بنابر این، در نگاه اول چنین به نظر می‌رسد که شرکت ها باید میان مزایای **BYOD** و به مخاطره افتادن امنیت داده‌های خود یکی را انتخاب کنند. اما از آنجا که مقدمات **BYOD** در واقع به نوعی به سازمان‌ها تحمیل می‌شود، باید راهی بیابند تا ضمن استفاده از مزایای آن، بتوانند بر چالش‌های امنیتی ناشی از آن فائق آیند. منظورم از تحمیل شدن **BYOD** این است که هر شرکت یا سازمان، با کارکنانی سر وکار دارد که هر کدام از ابزارهای همراه خود استفاده می‌کنند و مدیران سازمان نمی‌توانند از آن‌ها بخواهند که در ساعات یا در محیط کاری، ابزارهای همراه خود را کنار بگذارند و از دستگاه‌های شرکت استفاده کنند. با چنین استدلالی، بسیاری از سازمان‌ها تلاش می‌کنند تا با وضع مقرراتی برای استفاده از ابزارهای همراه کارکنان، از پراکندگی کارها و نشت داده‌ها تا حد ممکن جلوگیر کند.

چه باید کرد؟

1. نرم‌افزارهای مدیریت داده‌های موبایل یا Mobile Data Management) (MDM اولین گام در جهت تامین امنیت در پیاده‌سازی **BYOD** است. با استفاده از چنین نرم‌افزارهایی، تمامی دستگاه‌هایی که قرار است با شبکه شرکت در ارتباط باشند، ثبت (Register)، شناسایی و تائید (Verify) می‌شوند. چنین سیستم‌هایی، قابلیت‌های نظارت و فیلتر کردن، تشخیص و مقابله با نفوذ را فراهم می‌کنند.
2. سیاست‌های **BYOD** شرکت باید کاملا واضح و از پیش‌تعریف شده باشد تا بتواند مسئولیت‌های کارکنان را به آن‌ها آموزش دهد. این سیاست‌ها باید ساده و قابل فهم و در بازه‌های زمانی مانند هر سال، قابل به روزرسانی باشد. این سیاست‌ها باید شامل توضیحاتی روشن درباره خود برنامه، مقررات مربوط به رمزهای عبور، مالکیت داده‌ها و مواردی از این دست باشد.
3. سیاست های **BYOD** باید شامل راهنمایی‌ها و مقررات روشنی در باره حوادثی مانند گم یا دزدیده شدن دستگاه باشد. در چنین مواردی، باید مدیران شبکه به سرعت از حادثه مطلع شده و اقدامات لازم برای محافظت از داده‌ها را به عمل آورند.
4. به وجود آوردن مکانیزم‌های احراز هویت و رمز عبورهای قدرتمند، از ضروریات پیاده‌سازی موفق برنامه‌های **BYOD** است.
5. برای اجرای یک **BYOD** موفق، به روزرسانی نرم‌افزارها و firmwareها بسیار ضروری است. بر همین اساس، پشتیبان‌گیری منظم از داده‌های حساس می‌تواند خطرات این روش را کاهش دهد.
6. دستگاه‌های قفل‌بازشده یا جلبریک شده در چنین سیستمی قابل پذیرش نیستند.

شاید مهم‌ترین نکته در پیاده‌سازی موفق سیاست‌های **BYOD**، توجه به این نکته باشد که کارکنان شرکت درک روشنی از سیاست‌های شرکت در این زمینه داشته باشند و این، میسر نمی‌شود جز از طریق آموزش مستمر و ایجاد انگیزه در آن‌ها. کارکنان باید به این نتیجه برسند که بی‌توجهی به مقررات امنیتی در جهت حفاظت از داده‌ها، می

تواند کل مجموعه، منجمله شغل خود آن‌ها را با خطر روبرو کند.

تعادل، رمز پایداری

با پیدایش مفاهیمی مانند اینترنت اشیاء، پوشیدنی‌ها و کاشتنی‌های هوشمند، افراد به طور روزافزونی با یک‌دیگر و با موسسسات پیوند می‌یابند. تغییر به سمت تحرک و چابکی، استفاده از سیاست‌هایی مانند **BYOD** را طلب می‌کند. این امر به ویژه برای موسسات کوچک و متوسط اجتناب‌ناپذیر است. برای این که تیمی‌های چابک و قابل انعطاف داشته باشید، باید بتوانید از تمام امکاناتی که در اختیار دارید استفاده کنید. داشتن چنین تیم‌های کارآمدی می‌تواند برای هر شرکتی یک مزیت رقابتی به حساب آید. در عین حال، امنیت، به مانند تمام اعصار و قرون، چالشی مستمر و پایان‌ناپذیر است، به ویژه برای عصر ما که مرزهای جغرافیایی به تدریج در حال کم‌رنگ شدن هستند. پس، یکی از هنرهای مدیران برجسته در این است که بین استفاده از امکاناتی مانند **BYOD** و چالش‌های امنیتی ناشی از اجرای آن، تعادلی برقرار کنند

تاریخ انتشار:

06 اسفند 1394

نشانی منبع:
https://www.shabakeh-mag.com/opinion/2917/byod%D8%8C-%D8%AF%D8%A7%D8%AF%D9%87%E2%80%8C%D9%87%D8%A7%DB%8C-%D8%B3%D8%A7%D8%B2%D9%85%D8%A7%D9%86%D8%8C-%D8%A7%D8%A8%D8%B2%D8%A7%D8%B1%D9%87%D8%A7%DB%8C-%DA%A9%D8%A7%D8%B1%DA%A9%D9%86%D8%A7%D9%86