جایی که واقعیت و مدیریت ریسک با هم تداخل می‌کنند

درس‌هایی از هک‌شدن شبکه سونی

» منبع: مجله هکینگ » نویسنده: سیمون واکر، جواد مالک » ترجمه: احمد شریف‌پور

تاکنون مقالات زیادی به شبکه پلی‌استیشن سونی، PSN، اختصاص داده شده است که در پی نفوذ هکرها از کار افتاد. این رخداد به شدت کانون توجه همگان قرار گرفت و به سبب طرح سؤالات فراوان از سونی، مایه شرمندگی مدیران این شرکت شد. سؤالاتی که به برخی از آن‌ها هنوز هم پاسخ قانع‌کننده‌ای داده نشده است.

محافظت در برابر تمام مشکلات امنیتی یک محصول به سادگی امکان‌پذیر نیست؛ اما ارزیابی مناسب ریسک حداقل نشان خواهد داد که این مشکلات احتمالی چه خواهند بود و امکان تصمیم‌گیری آگاهانه را فراهم خواهد آورد. این موضوعی است که هم برای سازمان و هم برای شما به‌عنوان مصرف‌کننده بسیار مهم است. شاید شما استیو جابز یا استیو بالمر نباشید یا شرکتی که در آن مشغول کار هستید، ممکن است یک جامعه بازی آنلاین نداشته باشد و ممکن است که به فروش کنسول‌های بازی نپردازد؛ اما به یقین مصرف‌کننده کالاها و خدماتی هستید که دست‌کم امیدوارید «امنیت» داشته باشد. اگر پول خود را در بانک می‌گذارید، امید دارید که تا زمانی می‌خواهید آن را برداشت کنید، سر جایش باقی بماند. اما مهم‌ترین موضوع این است که به دلیل استفاده بسیار محصولات از عناصر و بخش‌هایی که بر مبنای فناوری کار می‌کنند، امنیت در حال تبدیل شدن به مقوله‌ای با اهمیت روزافزون است. به عنوان مثال، ممکن است شما امروزه از بانکداری آنلاین استفاده کنید.

در اتفاقی که برای سونی رخ داد، نکته‌های بسیاری وجود دارد که افراد چه از دید فنی و چه از دید تجاری می‌توانند از آن‌ها درس بگیرند. این رخداد به‌ویژه تأثیر فرهنگ‌هایی را با ارزیابی ریسک ضعیف به خوبی نشان می‌دهد. شاید برآورد شرکت‌ها از میزان نگرانی‌های مشتریانشان در زمینه‌های امنیتی و ریسک‌های تکنولوژیک، کمتر از حد واقعی آن باشد.

شبکه پلی‌استیشن

خدمات شبکه پلی‌استیشن سونی، از دید مشتریان پیشنهاد فریبنده‌ای به نظر می‌رسد. علاوه‌بر فراهم‌آوردن امکان رقابت آنلاین، مشتریان می‌توانند از طریق این شبکه به گشت‌وگذار در اینترنت پرداخته، به‌صورت آنلاین فیلم ببینند و بسیاری از کارهای دیگر را انجام دهند. نخستین جذابیت این شبکه در مجموعه بازی‌های قابل دانلود آن نهفته است. این بسته جذاب که کاربری ساده‌ای نیز دارد، در سراسر جهان ۷۷ میلیون کاربر (فقط ۳ میلیون نفر در انگلیس) را به خود جذب کرده است.

اما در پشت این شبکه چه می‌گذرد؟

نکته اول: دسترسی سریع به خدمات است که به طور معمول به هویت‌سنجی سریع و پرداخت‌های آنی و یکپارچه با سیستم تعبیر می‌شود و این خود به معنای ذخیره‌سازی اطلاعات مرتبط با کاربر (مثلاً شماره کارت اعتباری) در محل‌هایی با دسترسی ساده است. زمانی که شما چنین داده‌هایی را ذخیره کنید، چیزی در اختیار دارید که ارزش سرقت شدن را دارد.

نکته دوم: کاربر نهایی (فردی که در خانه با پلی‌استیشن بازی می‌کند) ممکن است تصور کند که محصول امنی را خریداری کرده، زیرا برای اطلاعات خود کلمه عبور تعریف کرده است. اما آنچه که نمی‌تواند ببیند، این است که زیرساختی که تمام این خدمات را پشتیبانی می‌کند، چندان امن نیست.

نکته سوم: اگر شما محصولی برای جوانان و افراد آشنا با فناوری عرضه می‌کنید، محصولی که باید به‌صورت جهانی قابل دسترسی باشد، شما در واقع در حال ایجاد یک نگاشت به جامعه افرادی هستید که بیشترین علاقه را به آزمایش فناوری‌های جدید دارند.

هیچ‌کدام از این موارد، موضوعاتی محرمانه و ناشناخته نبودند. پس چه چیزی مایه اشتباه شد؟

داستان سونی

بنا به اظهارات سونی، این رویداد نفوذی بود که از مکانی بیرون از مجموعه سونی صورت گرفته بود و به یقین به افشای بخش‌هایی از داده‌های کاربران منجر شده بود. بخش‌هایی نظیر نام کاربری، آدرس (شهر و ایالت و کدپستی)، کشور، آدرس پست الکترونیک، تاریخ تولد و کلمه عبور PSN از جمله داده‌های افشا شده بودند. علاوه بر این جزئیات به نظر می‌رسد که داده‌های بیشتری نظیر اطلاعات کارت‌های اعتباری و اطلاعات حساب‌های پایین دستی (نظیر حساب‌هایی که والدین ایجاد کرده و از طریق آن حساب‌های فرزندانشان را شارژ می‌کردند) نیز فاش شده‌اند. به یقین، گزارش‌های برخی مطبوعات نیز چنین مواردی را تأیید می‌کنند. توصیه سونی اتخاذ راهکارهای احتیاطی (مثلاً تماس با بانک و اعلام افشای اطلاعات کارت بانکی) است.

نخستین ادعاهای سونی درباره رهبری و پیاده‌سازی این حمله از طریق گروه هکری «ناشناس» (Anonymous) بلافاصله توسط این گروه رد شد. گروه هکری ناشناس به سرعت و به‌صورت رسمی دخالت در این عملیات را رد کرد. به نظر می‌رسد، این ادعا تنها تلاشی برای توجیه مشکل به‌وجود آمده بود که در هر صورت چندان پذیرفتنی نبود. ریشه اصلی این رخداد نتیجه تأثیر عملیات و اتفاقات بیرونی نبود، بلکه در (سیستم‌های امنیتی) خود سونی نهفته بود.

ارزیابی امنیت، بایدها و نبایدها

در تئوری، اصول پذیرفته‌شده‌ای وجود دارند که هرگاه سازمانی (دولتی) یا مجموعه‌ای تجاری قصد راه‌اندازی خدمات فناورانه جدیدی (مانند یک فروشگاه آنلاین) را داشته باشد، باید به آن‌ها پای‌بند باشد. خلاصه این اصول به این شرح است:

- سازمان‌ها باید در سیاست‌نامه‌ای مدون، اعلام کنند که محصول جدید به ارزیابی ریسک امنیتی نیاز دارد.
- در یکی از مراحل آغازین پروژه جدید، با متخصصان امنیتی سازمان مشورت شود تا آن‌ها اعلام کنند که کدام نمونه از خصیصه‌های امنیتی باید در محصول جدید گنجانیده شود.
- پیش از راه‌اندازی محصول، آزمایش‌های لازم برای اطمینان از پیاده‌سازی خواسته‌های متخصصان امنیت انجام شود. این مورد می‌تواند حتی شامل آزمایش نفوذ (هک اخلاقی) نیز باشد.
- هر مشکل یافته شده، گزارش شده و پیش از ارائه محصول به بازار برطرف شود.

اما در عمل قضیه بسیار متفاوت است. اگر سازمانی به این نتیجه برسد که سایر موارد (مثلاً عرضه سریع محصول به بازار) مهم‌تر از امنیت محصول است، ممکن است از این اصول تعدی‌کرده و از مراحل گفته‌شده صرف‌نظر کند.

مشتریان در اغلب موارد درباره «امنیت» به عنوان بخشی از محصولی که خریداری می‌کنند، پرس‌وجو نمی‌کنند. به نظر شما چه تعداد از نوجوانانی که مشتاق خرید PS3 هستند، واقعاً درباره امنیت جزئیات حساب‌های مالی والدین‌شان فکر می‌کنند؟ ممکن است متخصصان امنیت گاهی با یافته‌ها و مواردی روبه‌رو شوند که درک آن‌ها مشکل و بسیار پیچیده باشد یا به روشنی توصیف نشده باشد. همچنین ممکن است گاهی بسیار دیرتر از آن‌که بتوانند تغییری اساسی ایجاد کنند، به یک پروژه دعوت شوند.

آنچه شما در این مقاله خواهید آموخت:

- چرا ارزیابی ریسک مهم است؟
- چرا گاهی سازمان‌ها در این مورد اشتباه می‌کنند؟
- چگونه مشکلات امنیتی بر افراد (و نه فقط سازمان‌ها) اثر خواهند گذاشت؟
- گام‌هایی که باید برای حفاظت از داده‌های شخصی خود بردارید؟

آنچه باید بدانید:

- **ساده‌ترین تعریف ریسک:** رویدادی زیان‌آور به همراه احتمالی که به آن نسبت داده می‌شود.
- **ساده‌ترین تعریف ارزیابی ریسک:** فرآیند ارزیابی مواردی که ممکن است با مشکل روبه‌رو شود و میزان احتمال رخ دادن آن.

چشم‌انداز فرهنگی؛ تصمیم‌گیری در خلاء؟

در این مورد خاص فرهنگ تجاری حاکم بر سونی، ممکن است یکی از عوامل بسیار مهم جریان باشد. این نخستین‌باری نیست که سونی دست به یک بازی (حرکت) سریع زده و در آن شکست خورده است. در اکتبرسال ۲۰۰۵ این نکته مطرح شد که دیسک‌های موسیقی سونی برای «مدیریت حقوق دیجیتال» روتکیتی را روی کامپیوترهای کاربران نصب می‌کنند. یافتن و از بین‌بردن این روتکیت کار چندان مشکلی نبود و این کار مطابق قوانین بسیاری از

کشورها جرم محسوب می‌شد. این قضیه به صورت قابل بحثی کاربران را در معرض ریسک‌های امنیتی خطرناک قرار می‌داد.

آیا دلیل این امر به سادگی ارزش کمتر ملاحظات امنیتی نسبت به ملاحظات تجاری بود؟ شاید توسعه‌دهندگان مجبور به عرضه محصولی شده بودند که به‌صورت ذاتی از امنیت پایینی برخوردار بود یا حتی قابلیت‌های امنیتی در آن پیش‌بینی نشده بود. این اتفاق ممکن است به این دلیل رخ دهد که آن‌ها در این زمینه آموزشی ندیده‌اند یا شرح وظایف این توسعه‌دهندگان بدون ملاحظات امنیتی تعریف شده است.

اگر عرضه محصول به واسطه محدودیت زمانی تحت فشار باشد، دیگر برای آزمایش‌های سنگین امنیتی روی زیرساخت نگه‌دارنده محصول جایی وجود نخواهد داشت. به هر حال کاربر نهایی از امنیت برخوردار خواهد بود. چرا نگران چیز دیگری باشیم؟

اما از نقطه نظر فرهنگی هنوز مشکل دیگری نیز در زمینه تصمیم‌گیری وجود دارد. در سازمان‌های به شدت سلسله مراتبی، نیروی واقعی تصمیم‌گیرنده معمولاً تماماً در بالای هرم سلسله مراتب متمرکز شده‌است. سطحی که در آن معمولاً از متخصصان فنی خبری نیست و این متخصصان جایی در این سطوح ندارند. ارزیابی ریسک چندان آسان نیست و اگر به واقعیت‌ها و حقایق دسترسی نداشته باشید، دشوارتر هم خواهد شد. این امر باعث خواهد شد که مدیران رده بالا به جای ارزیابی میزان ریسک (که فرآیندی پردردسر و مستلزم درگیرشدن با جزئیات است) درباره اندازه آن «تصمیم بگیرند».

با این اوصاف، آیا مدیران سونی به عنوان یک سیاست کلی درباره همه محصولات یا فقط درباره این محصول اصلی و راهبردی، در زمینه امنیت دست به «تصمیم‌گیری» زده‌اند؟ چنین کاری به سادگی زمینه را برای رخدادهای بعدی فراهم خواهد کرد.

آیا ارزیابی ریسک به شیوه درست پیاده شده یا تنها میانبرهایی برای عبور سریع از مراحل مختلف تولید محصول برای رسیدن به مهلت زمانی خاصی بوده است؟ آیا شبکه به شیوه‌ای مناسب تفکیک شده بود تا بخش‌های مرتبط با بازی از بخش‌های مربوط به پرداخت‌ها مجزا شود؟ آیا برای آزمایش تمام و کمال سیستم زمان کافی اختصاص داده شده بود؟ بسیاری از شرکت‌ها با عرضه نسخه‌های بتا و فراهم آوردن امکان گزارش‌خطا برای کاربرانشان، از این مرحله به سرعت عبور می‌کنند. اگرچه این شیوه ممکن است ارزان و رضایت‌بخش به نظر برسد، اما در همه شرایط اقدامی درست و اصولی نخواهد بود.

درس‌هایی که آموخته شد

می‌توان به‌راحتی و با نسبت دادن ریشه‌های این اتفاق به بی کفایتی دست‌اندرکاران از آن گذشت. اما این کار ساده‌انگاری است و چندان مفید نخواهد بود. بنابراین، منعکس کردن برخی از بن‌مایه‌های اصلی چنین رخدادی، چه از دید یک شرکت و چه از دید یک فرد بی دلیل نخواهد بود.

چشم‌انداز شرکتی

زمانی که پلی‌استیشن ۳ به دست کاربر نهایی برسد، سونی در برابر هرگونه تغییر و دستکاری که کاربر در آن اعمال کند، تقریباً توانایی هیچ واکنشی را نخواهد داشت. بنابراین، هرگونه تمهیدات امنیتی که در داخل دستگاه تعبیه شده باشد، بی‌فایده خواهد بود. اگر شما محصول یا قطعه‌کدی را به مشتریانتان تحویل می‌دهید، تا چه حد می‌توانید مطمئن باشید که این محصول به هر شکلی، دستکاری نشود؟

همان‌گونه که هر جرم‌شناسی نیز به شما خواهد گفت، برای وقوع یک جرم به سه عامل وسیله، انگیزه و فرصت نیاز خواهد بود. یک پورتال آنلاین مانند شبکه پلی‌استیشن، یک سایت یا یک برنامه بانکداری با هدف فراهم کردن دسترسی برای کاربران تمام دنیا تولید می‌شود، به عنوان راه دسترسی به نوعی دارایی ارزشمند طراحی خواهد شد و بنابراین بی‌شک توسط عده‌ای مورد هجوم قرار خواهد

هکر PSN به‌دام افتاد

سه مظنونی که در حمله به شبکه PSN سونی دست‌داشته‌اند، توسط پلیس اسپانیا دستگیر شدند. به گفته پلیس دستگیرشدگان، رهبران محلی گروه هکری معروف Anonymous هستند. گروهی که به‌صورت واقعاً ناشناس فعالیت می‌کند و اعضای آن در سراسر دنیا پراکنده شده‌اند.

توجه پلیس اسپانیا در اکتبر گذشته به این سه نفر جلب شد، یعنی زمانی که آن‌ها با حمله به وب‌سایت وزارت فرهنگ اسپانیا به قوانین جدید این وزارت‌خانه در راستای افزایش مجازات دانلودهای غیرقانونی واکنش نشان دادند. با بررسی سوابق گفت‌وگوهای آنلاین (چت) و صفحات مختلف وب، پلیس رد حمله به شبکه PSN را تا سرور یکی از مظنونان دنبال کرد.

این سیستم همان سروری بود که چندین سایت دیگر از جمله سایت دو بانک اسپانیا، چندین سایت دولتی در اسپانیا، الجزایر، مصر، ایران و حتی سایت شرکت ایتالیایی Enel را که در زمینه انرژی فعالیت دارد، نیز از کار انداخته بود. اگر جرم این سه نفر ثابت شود، ممکن است به مجازاتی معادل سه سال زندان برای همکاری غیرقانونی در نفوذ به سایت‌های شخصی و سازمانی محکوم شوند. البته، هنوز

مشخص نیست که آیا این سه نفر یا حتی گروه هکری انانیموس تنها مهاجمان شبکه سونی (با خسارت تخمینی ۱۷۱ میلیون دلار) بوده‌اند یا این‌که گروه‌های دیگری نیز با انانیموس در این سرقت همکاری داشته‌اند.

گرفت. مسئله این نیست که آیا شما مورد حمله قرار خواهید گرفت یا خیر، بلکه مسئله اصلی این است که آیا قادر به تشخیص حمله، جلوگیری از آن و برطرف کردن بحران ناشی از حمله در زمانی معقول خواهید بود یا خیر.

با در نظر داشتن این نکته آخر، باید امنیت محصول را از ابتدا تا انتها مورد توجه قرار داد. همان‌گونه که برای سونی اتفاق افتاد، اگر زیرساخت نگه‌دارنده محصول شما مملو از حفره‌های امنیتی باشد، غیرقابل نفوذ بودن محصول شما هیچ فایده‌ای نخواهد داشت. یک هکر هیچ‌گاه همانند یک مدیر پروژه فکر نخواهد کرد. یک هکر به دنبال حفره‌های موجود در حصار دفاعی شما می‌گردد، نه این‌که نگران پروژه‌های فرعی باشد که هر یک بخشی از محصول نهایی شما را می‌سازند.

سونی هنگام مشخص‌شدن نفوذ به سیستم تصمیم گرفت، شبکه پلی‌استیشن را موقتاً از کار بیاندازد. سونی به عنوان یک سازمان این امکان را دارد که با استفاده از اندوخته‌هایش، کل شبکه را چند روز یا حتی چندین هفته و حتی به قیمت از دست دادن سود از کار بیاندازد. البته حتی سونی هم تا حد مشخصی از ضرر را تحمل خواهد کرد. اما اگر شما شرکتی هستید که تنها از طریق اینترنت با مشتریان خود سروکاردارید، آیا می‌توانید پس از انجام یک نفوذ، کل سیستم خود را آفلاین کنید؟ این مسئله بیشتر کسب‌وکارهای کوچک را تهدید خواهد کرد.

چشم‌انداز فردی

به حلقه ضعیف زنجیره دفاعی تبدیل نشوید. به عنوان مثال، بسیاری از افراد از کلمه عبور یکسانی در سیستم‌های مختلف استفاده می‌کنند. به همین دلیل، کلمه عبوری که برای شبکه پلی‌استیشن به کار می‌برند، همان کلمه عبوری است که از آن در ایمیل، بانکداری آنلاین، آمازون، Ebay و PayPal استفاده خواهند کرد و تمام این‌ها به این معنا است که اگر کلمه عبور شما در یکی از این سیستم‌ها مورد دستبرد قرار بگیرد، ممکن است به روش‌های گوناگونی تحت تأثیر قرار بگیرید و بیشترین تأثیر چنین مشکلاتی به طور مستقیم گریبان‌گیر خود شما خواهد بود؛ زیرا شما باید برای مسدود کردن حساب‌ها یا لغو اشتراک‌ها به بانک یا سایت‌های مختلف مراجعه کنید. چه تعداد از والدین هنگام ثبت مشخصات کارت اعتباری خود در PSN به این مسائل اندیشیده بودند؟

پیش از به اشتراک گذاشتن اطلاعات‌تان در شرکت‌های آنلاین به دقت فکر کنید. تا چه حد مطمئن هستید که آن‌ها از اطلاعات شما به درستی محافظت می‌کنند؟ آیا در این مورد سؤال کرده‌اید؟ حتی اگر شرکتی محصول یا خدمات ارزان قیمتی را ارائه می‌کند، به اندازه یک بانک ملزم به حفاظت از کلمه عبور و اطلاعات شما خواهد بود. شما با پرسیدن این سؤال که «محصول آنلاین شما تا چه اندازه امن است؟» لطف بزرگی در حق همه خواهید کرد. این سؤال به شرکتی که شما در حال خرید از آن هستید، نشان خواهد داد که امنیت مقوله مهمی است.

به خاطر داشته باشید که به صورت قانونی حق با شما است. در بسیاری از کشورها و به‌ویژه در اتحادیه اروپا قوانینی درباره نحوه جمع‌آوری، ذخیره، پردازش و امن نگه داشتن اطلاعات شخصی افراد وضع شده است.

به یقین، چنین قوانینی به تنهایی مانع از بروز مشکلات امنیتی نخواهند شد، زیرا که قانون به تنهایی از وقوع جرم جلوگیری‌نخواهد کرد. اما به شرکت‌ها و سازمان‌ها یادآوری خواهد کرد که باید ملاحظات شما را جدی بگیرند.

آینده

سونی سرانجام از بحران ناشی از این حادثه بیرون خواهد آمد. شبکه پلی‌استیشن دوباره آنلاین خواهد شد و کاربران ممکن است گاهی به یاد هفته‌هایی بیفتند که مجبور بودند بدون بازی‌های آنلاین سر کنند.

هرچه نفوذهای بیشتری رخ دهد، مشتریان بیش از پیش انتظار خواهند داشت که امنیت به یکی از خصوصیات کلیدی محصول یا خدمات شما تبدیل شود. به هرحال داده‌های آن‌ها است که در معرض خطر قرار دارد و آن‌ها هستند که باید دردسرهای ناشی از مسدود کردن حساب‌ها و... را تحمل کنند. این ملاحظات باید در متن تصمیم‌گیری‌های تجاری مرتبط با امنیت دخیل شود، نه این که تنها به عنوان ماده‌ای از حقوق قانونی مصرف‌کنندگان در قراردادهای فروش یا ارائه خدمات ذکر شود. به نظر می‌رسد، رسانه‌ها هم همین نظر را داشته و بیش از پیش مایل هستند داستان‌هایی درباره مسائل و مشکلات امنیتی موجود منتشر کنند.

صنایع خودروسازی در چند دهه گذشته بیش از هر چیز بر امنیت خودروها تأکید داشته‌اند. اکنون و تنها بعد از گذشت چند دهه، هنگامی که یک راننده درگیر یک تصادف می‌شود، دیگر مطمئن است که کمربندهای ایمنی، کیسه‌های هوا و سایر تمهیدات ایمنی خودرو او را از مرگ یا جراحات شدید محافظت خواهد کرد. شرکت‌های فعال در دنیای IT نیز باید اعتماد کاربرانشان را جلب‌کنند و به آن‌ها اطمینان دهند که حتی در صورت بروز هر مشکلی داده‌های آن‌ها در امان خواهد ماند. نت‌وست (Natwest) یکی از بزرگ‌ترین بانک‌های انگلیس و جزئی از گروه RBS است. لحاظ شدن معیارهای امنیتی در موافقت‌نامه کاربران نت‌وست، یکی از مثال‌های مناسب نگاه به امنیت به عنوان جزئی از ارزش یک محصول است. این سند (موافقت‌نامه کاربران نت‌وست) که به‌صورت سالانه منتشر می‌شود، کارایی سازمان را در برابر مجموعه‌ای از آزمایش‌ها به تفصیل شرح می‌دهد و با تبلیغات تلویزیونی نیز حمایت می‌شود. در آخر، تأثیر بلند مدت نقص‌های امنیتی را در خاطر داشته باشید. اگر PSN امن نبوده، چه محصولات، خدمات یا زیرساخت‌های دیگری از سونی اکنون زیر ذره‌بین قرار گرفته است؟ و زمانی که تمام این نوجوانان چهارده ساله تصمیم بگیرند خرید فناورانه بعدی خود را انجام دهند، چه خواهد شد؟

درباره نویسندگان

۱. سیمون واکر: در زمینه امنیت اطلاعات و در عرصه‌هایی نظیر امور مالی، دولتی، پخش محتوا و سایر بخش‌های فناوری‌محور، بیش از دوازده سال سابقه دارد. وی در شرق اروپا، آفریقای جنوبی و ترکیه کار کرده است. سیمون به راهبردی بودن و نحوه مدیریت امنیت اطلاعات توجه ویژه‌ای دارد. او یکی از نویسندگان گزارش‌های امنیتی مختلف بوده و مقاله‌هایی را در نشریه‌های اروپا و خاورمیانه به چاپ رسانده است. سیمون که قبلاً عضو CLAS (سرنام CESG Listed Advisor Scheme) بوده، اکنون در مدرسه تجارت هنلی (Henley) به تحصیل در رشته MBA مشغول است.

۲. جواد مالک: با بیش از یازده سال تجربه که بیشتر آن در بانک‌های معتبر جهانی بوده است، از متخصصان امنیت اطلاعات و مشاور ارشد امنیت در کوانتاینیا (Quantainia) است. وی که به عنوان یکی از مدافعان افزایش آگاهی عمومی شرکت‌ها و افراد در زمینه امنیت به شمار می‌رود، مقاله‌ها و ویدیوهای متعددی را در زمینه امنیت اطلاعات منتشر کرده است. جواد مالک، مدارک CISSP و SANS GIAC را کسب کرده و یکی از بنیان‌گذاران سکیوریتی‌بی‌سایدز (Security B-Sides) در لندن است.