طوفان «فیشینگ پیامکی» در بحران کرونا

فیشینگ پیامکی (Smishing) از زمان شیوع کووید۱۹ به یک تجارت پررونق برای مجرمان سایبری تبدیل شده است و انتظار می‌رود که این تهدید، ادامه‌دار باشد

میترا جلیلی
خبرنگار

«گوگل پلی» در تازه‌ترین گزارش خود از وجود تعدادی اپلیکیشن مخرب در این فروشگاه خبر داده و یادآور شده است که این اپ‌ها در واقع میزبان تروجان‌ها و بدافزارهایی هستند که با آلوده کردن گوشی‌های اندرویدی، اطلاعات کاربران را به سرقت می‌برند و تاکنون ازطریق فیشینگ پیامکی (Smishing)، به داده‌های مالی و بانکی میلیون‌ها نفر درجهان دسترسی پیدا کرده‌اند. کارشناسان معتقدند این نوع فیشینگ از زمان شروع همه‌گیری کووید۱۹ به یک تجارت پررونق برای مجرمان سایبری تبدیل شده است و البته انتظار می‌رود که این تهدید، ادامه دار باشد؛ درحالی که تاکنون باج‌افزارها سهم عمده حملات سایبری را به خود اختصاص داده بودند اما حالا به نظر می‌رسد مجرمان سایبری تصمیم گرفته‌اند در حملات هکری خود، از فیشینگ پیامکی بیشترین استفاده را ببرند و حتی برخی، از این مدل فیشینگ به عنوان یک طوفان بزرگ یاد می‌کنند.

زیان ۵۰ میلیون دلاری اسمیشینگ

فیشینگ پیامکی که به نام smishing نیز شناخته می‌شود هربار با ویژگی‌های جدیدی ظاهر می‌شود. طبق گزارش اف بی آی، در سال ۲۰۲۰ حملات Smishing تنها برای کاربران امریکایی، زیان ۵۰ میلیون دلاری داشته و انتظار می‌رود که این رقم در سال ۲۰۲۱ افزایشی چشمگیر یابد. کمپانی امنیت سایبری Proofpoint نیز گزارش داده که حملات فیشینگ پیامکی در امریکای شمالی در سه ماهه سوم سال جاری افزایش ۳۰۰ درصدی نسبت به مدت مشابه سال گذشته داشته و البته این رقم برای کاربران بریتانیایی، ۷ برابر شده است؛ البته این نوع فیشینگ تنها مختص گوشی‌های اندرویدی نیست و گوشی‌هایی با سیستم عامل IOS نیز هدف این حملات قرار می‌گیرند اما میزان موفقیت مجرمان سایبری از طریق گوشی‌های اندرویدی بسیار بیشتر از آیفون بوده است به همین دلیل هم در زمینه چنین حملات سایبری بیشتر به کاربران دستگاه‌های اندرویدی هشدار داده می‌شود.

در گزارشی که بتازگی توسط کمپانی ThreatFabric تهیه شده نیز بدافزار FluBot مورد توجه قرار گرفته و آمده است که بتازگی شاهد انتشار گسترده بدافزار FluBot و حملات اسمیشینگ ناشی از آن در جهان هستیم. این بدافزار که پیش از این نیز در آوریل ۲۰۲۱ میلیون‌ها گوشی اندرویدی در سراسر جهان را آلوده کرده بود، این بار به عنوان یک جاسوس‌افزار و در قالب فیشینگ پیامکی (Smishing)، کاربران جهان را نشانه رفته و البته فنلاندی‌ها بیش از همه در معرض این بدافزار قرار گرفته‌اند. FluBot و سایر بدافزارهایی که به فیشینگ پیامکی می‌پردازند دائم تغییر رویه می‌دهند و شناسایی آنها چندان راحت نیست. به عنوان مثال در فوریه، مهاجمان سایبری در بریتانیا بازگرداندن مالیات اضافی پرداخت شده توسط کاربران را دستاویز قرار داده و در قالب پیامک‌های جعلی، مردم را تطمیع کردند که با کلیک بر لینک مربوطه، مبلغ مالیات‌های اضافی را پس بگیرند درحالی که عملاً هکرها به smishing پرداختند.

از بسته پستی تا احضاریه دادگاه

این بار بدافزار «FluBot» در کشورهای اسپانیا، ایتالیا، بریتانیا، آلمان، نیوزیلند و... به گوشی‌های اندرویدی کاربران حمله کرده است. چنین حمله‌ای حتی سبب شد تا در فنلاند وضعیت فوق‌العاده سایبری و هشدار اعلام شود. این بدافزار در فنلاند و دیگر کشورهای جهان با ارسال پیامک‌های مخرب، کاربران را هدف گرفته و آنها را متقاعد می‌کند که

گیرمو

هنگام ارسال بسته پستی، در محل حضور نداشته‌اند و با کلیک بر پیوند ارائه شده در پیامک، به ردیابی و پیگیری وضعیت بسته پستی خود بپردازند. حتی کاربرانی که منتظر هیچ بسته پستی نبوده‌اند بدون توجه به مسائل امنیت سایبری، بر لینک مربوطه کلیک می‌کنند. بلافاصله یک برنامه فیشینگ دانلود می‌شود که عملاً بدافزار FluBot را در خود جای داده است. طبق گزارش شرکت امنیت سایبری Proofpoint، هنگامی که FluBot مجوزهای لازم را از قربانیان ناآگاه دریافت کرد، به کل دستگاه دسترسی پیدا می‌کند و به عنوان جاسوس‌افزار، اطلاعات همه کارت‌های بانکی و اعتباری کاربر را به دست می‌آورد و همچنین با ارسال پیامک برای افرادی که نام آنها در لیست مخاطبان قربانی قرار گرفته، آنها را نیز هدف این حمله بدافزاری قرار می‌دهد. در فیلیپین هم این بدافزار افراد جویای کار را هدف قرار داده است و با دسترسی به اطلاعات و داده‌های سامانه‌های اشتغال در این کشور، جوانان را هدف گرفته‌اند. کاربران به محض دریافت پیامک و کلیک بر لینک مربوطه، در دام هکرها می‌افتند و همه اطلاعات بانکی و شخصی آنها به سرقت می‌رود درحالی که منتظر دریافت پیشنهاد شغلی هستند. در ایران نیز شاهد smishing بوده‌ایم و این حملات با پیام کوتاه از یک سیستم اطلاع‌رسانی قضایی الکترونیکی آغاز می‌شود که به قربانی اطلاع می‌دهد شکایتی علیه وی انجام شده است. با کلیک بر لینک مربوطه، قربانی به صفحه‌ای جعلی هدایت می‌شود و درست در همین زمان یک فایل apk مخرب دانلود می‌شود. در این صفحه از قربانی خواسته می‌شود شماره همراه و کارت ملی خود را وارد کند و هزینه اندکی بین ۲۰ هزار تا ۵ هزار ریال واریز کند. پس از انجام تراکنش، پیام «خطای پرداخت» نمایش داده می‌شود و عملاً مهاجمان سایبری شروع به کلاهبرداری‌های مالی می‌کنند چراکه حالا دیگر بدافزار فعال شده است و کاربر با وارد کردن اطلاعات بانکی خود برای واریز این مبلغ، عملاً همه اطلاعات بانکی خود را در دسترس هکرها قرار داده است.

یک «درپشتی» پردردسر

اما عملکرد این بدافزارها چگونه است؟ هکرها با انتخاب قربانیان خود، برای آنها پیامک‌های مهندسی شده ارسال می‌کنند؛ با ارسال این پیامک‌ها عملاً بدافزار اندرویدی به صورت چراغ خاموش، یک درپشتی (backdoor) در گوشی کاربر ایجاد می‌کند و عملکرد دستگاه را در اختیار می‌گیرد. محققان از گستردگی این حمله‌های فیشینگ پیامکی و همچنین میزان بالای ارقام کلاهبرداری شده، متعجب هستند و آن را قابل توجه می‌دانند. موضوع جالب اینجاست که بدافزار بلافاصله تمام پیامک‌های قربانی را به یک سرور خاص ارسال می‌کند و با این نوع دسترسی به داده، مهاجمان می‌توانند احراز هویت دومرحله‌ای (2FA) را نیز در حساب‌های مالی دور بزنند و از حساب‌ها برداشت کنند.

اگر گوشی شما به Flubot آلوده شد یا احتمال آلوده شدن آن را می‌دهید چه باید بکنید؟ ساده‌ترین راه این است که به لینک‌های ارائه شده در همه پیامک‌ها اعتماد نکنید و قبل از اطمینان از درستی آن، هرگز بر لینک مربوطه کلیک نکنید تا از هک شدن و لو رفتن اطلاعات بانکی شما جلوگیری شود. موضوع مهم دیگر این است که این بدافزار را از گوشی خود حذف کنید. هرچند این ویروس را می‌توان به صورت دستی از گوشی‌ها پاک کرد اما بهترین راه برای پاک کردن آن، بازگرداندن گوشی به تنظیم مجدد کارخانه است. به همین دلیل هم بهتر است همیشه از داده‌های گوشی خود بکاپ داشته باشید تا براحتی بتوانید در چنین شرایطی، گوشی خود را ریست کنید.

وزیر ارتباطات و فناوری اطلاعات خبرداد

موافقت رئیس جمهور با بازنگری تقسیم کار در حوزه امنیت سایبری

وزیر ارتباطات و فناوری اطلاعات، ضعف امنیت سایبری را پاشنه آشیل تحقق دولت هوشمند و توسعه فناوری اطلاعات در کشور عنوان کرد و از موافقت رئیس جمهور با تغییر و بازنگری تقسیم کار در حوزه امنیت سایبری خبر داد.

به گزارش «ایران»، عیسی زارع‌پور در جلسه تکریم و معارفه مدیران سابق و جدید سازمان فضایی ایران و بازرسی، نظارت مدیریتی و پاسخگویی به شکایات و معارفه نماینده ویژه وزیر ارتباطات در امور امنیت فاوا و نیز مشاور وزیر در تعامل با نیروهای مسلح، با اشاره به اهمیت حوزه فضایی و عنایت و اشراف رهبر معظم انقلاب به این حوزه، گفت: امیدواریم با حمایت تمام بخش‌ها و حرکت مجاهدانه بتوانیم صنعت فضایی را به ریل شتابان گذشته برگردانیم.

وزیر ارتباطات و فناوری اطلاعات درباره انتصاب نماینده ویژه خود در امور امنیت فاوا با اشاره به اینکه این حوزه نیاز به جراحی دارد، گفت: اگر به این حوزه توجه جدی نشود می‌تواند پاشنه آشیل دولت هوشمند و توسعه فناوری اطلاعات باشد ؛تقسیم کاری که در این حوزه در کشور انجام شده شفاف و کارآمد نیست و باید تغییر کند. وی با اشاره به موافقت رئیس جمهور با تغییر و بازنگری تقسیم کار در حوزه امنیت سایبری، افزود: کار ویژه نماینده وزیر ارتباطات و فناوری اطلاعات در امور امنیت فاوا، تهیه پیشنهادها و راهکارهای مناسب برای این حوزه است که باید بخش‌های مختلف وزارتخانه برای این موضوع همکاری کنند. وزیر ارتباطات و فناوری اطلاعات افزود: اعتقاد دارم مسیرهای میان‌بری برای رسیدن به اهداف بزرگ حوزه فضایی وجود دارد که باید به آنها دست پیدا کنیم. زارع‌پور با اشاره به بودجه حوزه فضایی برای سال آینده، تصریح کرد: با وجود زیرساخت‌های لازم و نیروی انسانی متخصص و متعهد در این حوزه، می‌توانیم صنعت فضایی را به صنعتی مترقی و پیشرفته برسانیم. زارع‌پور درباره انتصاب مشاور وزیر در تعامل با نیروهای مسلح نیز گفت: این انتصاب با هدف استفاده از ظرفیت نیروهای دفاعی کشور در پیشبرد مأموریت‌های وزارت ارتباطات انجام شده است؛ چون معتقدم باید انرژی همه ارکان نظام برای تحقق مأموریت‌های مربوط به شبکه ملی اطلاعات و صنعت فضایی کشور به کار گرفته شود. در پایان این جلسه وزیر ارتباطات و فناوری اطلاعات از مرتضی براری رئیس سابق سازمان فضایی کشور و حمیدرضا رضوانی‌پور رئیس سابق مرکز بازرسی وزارت ارتباطات قدردانی کرد. وی همچنین احکام حسن سالاریه رئیس سازمان فضایی کشور، علی بحرینی رئیس مرکز بازرسی، نظارت مدیریتی و پاسخگویی به شکایات، امیر محمدزاده لاجوردی، نماینده ویژه وزیر در حوزه امنیت فاوا و محمد مهدی نژاد نوری مشاور وزیر در تعامل با نیروهای مسلح را ابلاغ کرد.

اخبار

طراحی سکوی تشخیص اخبار جعلی در شبکه‌های اجتماعی

رئیس پژوهشگاه ارتباطات و فناوری اطلاعات از طراحی و توسعه نمونه اولیه سکوی تشخیص اخبار جعلی در شبکه‌های اجتماعی خبر داد.

به گزارش «ایران»، وحید یزدانیان با بیان اینکه آگاهی، پیشگیری و مقابله با تبعات ناخوشایند محتوا در شبکه‌های اجتماعی از ضروریات جوامع امروزی به حساب می‌آید، گفت: بی‌تفاوتی نسبت به این محتواها، ممکن است بحران‌هایی ایجاد کند که رفع آنها امکان‌پذیر نبوده یا مستلزم هزینه‌های گزاف باشد. وی ادامه داد: گاهی انتشار اطلاعات نادرست در فضای مجازی تهدید خاصی به‌حساب نمی‌آید و مثلاً با انگیزه سرگرمی و مزاح، محتوای نادرستی تولید و منتشر می‌شود و اثر طولانی مدتی ندارد، اما در مواردی محتواهای نادرست می‌توانند به‌صورت هدفمند و تأثیرگذار در سطح ملی و به‌منظور بر هم زدن نظم اجتماعی، امنیت، اقتصاد، تخریب اشخاص حقیقی یا حقوقی و امثال آنها باشند. وی خاطرنشان کرد: در این پروژه ضمن مروری گذرا بر این مباحث، روش‌های مبتنی بر هوش مصنوعی برای شناسایی اخبار مشکوک به جعلی بودن، مورد تمرکز بیشتری قرار گرفت و ضمن بررسی تنوعی از روش‌های مبتنی بر هوش مصنوعی، برخی از آنها پیاده‌سازی شد یا در حال انجام است. رئیس پژوهشگاه ارتباطات، نتایج حاصله را مثبت ارزیابی کرد و گفت: برای تحقق این امر از روش‌های مبتنی بر استخراج ویژگی‌های نوشتاری، روش‌های مبتنی بر کیسه کلمات n-gram ،(Bag of Words)، روش‌های مبتنی بر یادگیری عمیق و روش‌های مبتنی بر الگوی انتشار در شبکه استفاده می‌کنیم.

حذف خودکار همه پیام‌های واتس‌اپ امکانپذیر شد

کاربران واتس‌اپ می‌توانند گزینه پیام‌های محو شونده را برای همه پیام‌های جدیدی که ارسال و دریافت می‌کنند به‌صورت پیش فرض فعال کنند.

به‌گزارش ایسنا، سرویس پیام رسان واتس‌اپ گزینه‌ای را عرضه کرد که به کاربران امکان می‌دهد حذف خودکار پیام‌ها را به‌صورت پیش فرض برای همه مکالمات جدید فعال کنند. پیش از به‌روزرسانی جدید، کاربران باید به‌صورت دستی گزینه پیام‌های محو شونده را برای هر مکالمه جدید فعال می‌کردند. واتس‌اپ همچنین علاوه بر گزینه هفت روز که سال گذشته در زمان معرفی قابلیت پیام‌های محو شونده ارائه کرده بود، به‌کاربران گزینه برای حذف خودکار پیام‌هایشان پس از ۲۴ ساعت یا ۹۰ روز را می‌دهد. زفیر خان، مدیر محصول واتس‌اپ در مصاحبه‌ای با تک کرانچ گفت: تیم واتس‌اپ هنگام توسعه گزینه‌های جدید، بازخوردهای کاربران را دریافت کرده است.

وی خاطرنشان کرد: اگر یکی از طرفین گفت‌وگو گزینه موقتی را فعال کرده باشد، پیام‌ها پس از یک مدت معین حذف خواهند شد. واتس‌اپ این گزینه را برای همه پیام‌های گروه فعال کرده و در زمان ایجاد گروه امکان انتخاب چنین گزینه‌ای را فراهم می‌کند. حریم خصوصی همواره برای واتس‌اپ اساسی بوده است و ما گزینه موقتی بودن را استاندارد نوظهور جدیدی در پیام‌رسانی می‌دانیم. بر اساس گزارش تک کرانچ، مارک زاکربرگ، مدیرعامل فیس‌بوک که شرکت مادر واتس‌اپ است، در پستی در فیس‌بوک اعلام کرد لزومی ندارد همه پیام‌ها برای همیشه باقی بمانند.

پایان پشتیبانی انگلیس از 2G و 3G در ۲۰۳۳

دولت انگلیس اعلام کرد تا سال ۲۰۳۳ میلادی پشتیبانی از سرویس‌های موبایل 2G و 3G را پایان می‌دهد تا امواج رادیویی برای نسل 5G و 6G را ارائه کند.

به گزارش مهر، «نادین دوریس» وزیر فرهنگ انگلیس در این باره گفت: 5G هم اکنون زندگی مردم و کسب و کارها را دگرگون کرده است چرا که این فناوری، مردم را سریع‌تر به یکدیگر مرتبط می‌کند و سبب می‌شود کسب و کارها پربازده‌تر باشند. وی ادامه داد: ما ۵۰ میلیون پوند دیگر در حوزه ارتباط موبایل در انگلیس سرمایه‌گذاری می‌کنیم تا تضمین شود شبکه‌های مخابراتی ما اکنون و در آینده ایمن هستند. بودجه مذکور به پروژه‌های «pen Radio Access Networks» تخصیص می‌یابد و درحالی اعلام می‌شود که دوریس با همتای امریکایی خود دیدار می‌کند. «دوریس» در ادامه افزود: با پایان پشتیبانی از 2G و 3G، این روند ورود تولیدکنندگان تجهیزات جدید به بازار را تسهیل می‌کند زیرا آنها مجبور نخواهند بود از فناوری‌های قدیمی پشتیبانی کنند.

وب سایت‌های مشهور جهان از کار افتادند

یک اختلال گسترده در خدمات کلود شرکت آمازون باعث شد دهها سایت مشهور و پخش آنلاین فیلم و ویدیو مختل شوند.

به گزارش مهر، از جمله مهم‌ترین سایت‌های مختل شده می‌توان به نتفلیکس، دیزنی پلاس، رابین هود و تعداد زیادی از اپلیکیشن‌های وابسته به خدمات کلود آمازون اشاره کرد. نکته جالب اینکه اختلال یادشده باعث شد حتی تعدادی از وب سایت‌های تجارت الکترونیک آمازون نیز از دسترس خارج شوند و این رویداد در آستانه تعطیلات کریسمس موجب ناخشنودی بسیاری از کاربران شده است. آمازون با صدور بیانیه‌ای از بازگشت بسیاری از خدمات خود به حالت عادی خبر داده و افزوده که در تلاش است سایر خدمات خود را به حالت عادی بازگرداند. دوربین‌های امنیتی Ring آمازون، برنامه بانکداری تلفن همراه Chime و جاروبرقی روباتیک iRobot که از خدمات کلود آمازون استفاده می‌کنند هم طبق گزارش‌های درج شده در صفحات شبکه‌های اجتماعی دچار مشکل شدند. نتفلیکس که تقریباً تمام زیرساخت‌های خود را روی خدمات کلود آمازون مستقر کرده، به‌دنبال وقوع این اختلال ۲۶ درصد از ترافیک خود را از دست داد. آمازون مدعی شده که این قطعی مربوط به برخی سخت افزارهای شبکه بوده و به رابط برنامه‌نویسی آمازون و مجموعه‌ای از پروتکل‌ها که برای ساخت و یکپارچه‌سازی نرم‌افزارهای کاربردی استفاده می‌شود، مرتبط است.

نگاه ترفند

اشتراک رمز وای‌فای از طریق دستگاه اندرویدی

اگر یک رمز عبور فوق‌العاده امن برای وای‌فای خود تنظیم کرده‌اید که گفتن آن به افرادی که می‌خواهند به وای‌فای شما متصل شوند، فرایندی زمان‌بر است، می‌توانید رمز عبور وای‌فای خود را در اندروید از طریق کد QR به اشتراک بگذارید.

به‌گزارش ایسنا، امروزه از هر پنج نفر، سه نفر شبکه وای‌فای شخصی در خانه و محل کار خود دارند. این روزها بویژه در بحران کرونا، داشتن اتصال وای‌فای ضروری شده است. با این حال، مشکل داشتن وای‌فای شخصی این است که همه می‌خواهند به شبکه شما متصل شوند. هر بار که دوستی به خانه شما می‌آید، مجبور می‌شوید رمز عبور وای‌فای خود را به او بگویید. این فرایند آسان به‌نظر می‌رسد، اما زمان‌بر است و گاه ممکن است آزاردهنده باشد. همچنین، اگر یک رمز عبور فوق‌العاده امن برای وای‌فای خود تنظیم کرده باشید، ممکن است دوستانتان چندین بار تلاش کنند تا رمز عبور را درست دریافت کنند. دانستن روش صحیح به اشتراک‌گذاری رمزهای عبور وای‌فای در اندروید می‌تواند یک صرفه‌جویی خوب در زمان باشد، بخصوص زمانی که عجله دارید. آن‌طور که وب‌سایت تک‌وایرال گزارش می‌دهد، اندروید ۱۰ روشی بهتر و ساده را برای به اشتراک گذاشتن رمز وای‌فای خود با دیگران ارائه داده است. اندروید به‌شما این امکان را می‌دهد که جزئیات وای‌فای خود را به‌همراه نام شبکه، رمز عبور و تنظیمات شبکه از طریق کد QR به اشتراک بگذارید. شما فقط باید کد QR را برای شبکه خود ایجاد کنید و دوستانتان هم این کد را اسکن کنند. پس از اسکن، آنها به شبکه وای فای شما متصل خواهند شد. برای انجام این کار باید مراحلی را دنبال کنید. اول از همه، در گوشی هوشمند اندرویدی خود روی تنظیمات ضربه بزنید. در تنظیمات، روی «اتصالات» و سپس روی «وای‌فای» ضربه بزنید. اکنون روی دکمه چرخ دنده کوچک روبه‌روی نام WiFi ضربه بزنید. با این کار صفحه شبکه باز می‌شود. گزینه کد QR را در پایین صفحه خواهید دید. روی آن ضربه بزنید. کد QR روی صفحه نمایش داده می‌شود. حالا از دوستتان بخواهید دوربین را باز کند و اسکنر کد QR را روشن کند. اکنون دوربین را روی کد QR قرار دهید تا به شبکه WiFi متصل شوید. اگر گوشی دوست شما اسکنر کد QR ندارد، از او بخواهید از برنامه Google Lens استفاده کند. به این ترتیب می‌توانید رمزهای عبور وای فای را در اندروید به اشتراک بگذارید.

گنجاندن جرم شناسی دیجیتال و شبکه در سند سایبری

مرتضی نکویی
کارشناس امنیت سایبری

تقویت زیرساخت‌های مانیتورینگ در جهت بهبود شناسایی تهدیدات و توانایی بیشتر در جرم شناسی دیجیتال و شبکه پس از وقوع رخدادها و حوادث اخیر، بازنگری سند نظام ملی پیشگیری و مقابله با حوادث فضای مجازی بسیار مفید خواهد بود. ولی اینکه چه اصلاحاتی لازم است در آن صورت پذیرد که پاسخگوی نیازهای ما باشد یا حداقل در جهت بهبود چگونگی رویارویی با حوادث امنیتی یا پیشگیری از وقوع آنها عمل کند، بسیار حائز اهمیت است اما به دلیل گستردگی چالش‌ها و محرمانه بودن سند و منتشر نشدن آن خیلی نمی‌توان در این باره نظر داد.

اما به‌صورت کلی می توان گفت که مراکز CSIRT (رسیدگی به حوادث امنیت رایانه‌ای) و CERT (گروه پاسخگویی رخداد امنیتی) مراکزی هستند که در خصوص رسیدگی به رخدادهای امنیتی کامپیوتری فعالیت می‌کنند و باید فعال‌تر شوند و قبل از وقوع حادثه هشدارها را دریافت کرده و به نهادها و دستگاه‌ها اطلاع دهند.

در زمینه مدیریت، رسیدگی و پاسخگویی به رخدادها، استانداردها و کتاب‌ها و ژورنال‌های متعددی تدوین و منتشر شده که بکارگیری جدی آنها می‌تواند تغییرات چشمگیری در خصوص نحوه برخورد ما با رخدادها داشته باشد. نگاه جزء به کل در حوزه امنیت سایبری هم می‌تواند به ما بقبولاند که عزم جدی تری در این خصوص لازم است و هر سازمانی باید دارای حداقل مرکز عملیات امنیت (soc) متشکل از (راهکارهای امنیت اطلاعات و مدیریت رویدادها) siem و زیرساخت‌های هوشمند نظارتی و کنترلی باشد و تیم‌های cert سازمان‌های مادر با رصد لحظه‌ای و بلادرنگ رخدادها و حوادث، نسبت به آنها واکنش سریع نشان دهند. متأسفانه بسیاری از ارگان‌های کشور که مثل تار عنکبوت به هم متصل هستند، حتی حوصله توجه به مباحث امنیت اطلاعات را ندارند. بنابراین انتظار می‌رود حداقل در کوتاه مدت چنین اقدام‌هایی را در دستور کار خود قرار دهند.

مقوله امنیت اطلاعات بسیار گسترده و متشکل از چالش‌های بسیار متعدد و پیچیده‌ای است. از یکسو نمی‌توان استفاده از تکنولوژی و فناوری‌های تولید شده از سوی غرب یا کشورهای جهان اول را نادیده گرفت از سوی دیگر هم نمی‌توان در کوتاه مدت به خودکفایی در حوزه‌های بسیار پیچیده‌ای از قبیل تولید کوچک‌ترین قطعات سخت افزاری دست یافت. بنابراین همان‌طور که گفته شد باید نگاه جزء به کل را در نظر بگیریم، چرا که ما از کل خبر داریم و آن هم تأمین امنیت است. امنیت اطلاعات مبحثی است که با قطعه قطعه و جزء به جزء تکنولوژی و حتی فراتر از آن و همچنین پیش پا افتاده‌ترین مباحث از جمله نیروهای انسانی سر و کار دارد و رسیدگی به تمام آنها نیازمند آن است که ابتدا به روش دقیق و منسجمی در این خصوص دست یابیم و پس از آن دست به تدوین اسناد مرجع بزنیم.

از سوی دیگر باید به مباحث مانیتورینگ و رصد دقیق زیرساخت‌ها و نفوذ و استخراج اطلاعات‌مان توجه کنیم و همچنین دنبال جرم شناسی دیجیتال و شبکه و غیره در سند باشیم و از تکنیک‌هایی استفاده کنیم که بتوانیم ردپایی از چرایی و چگونگی حملات سایبری به زیرساخت‌ها به‌دست آوریم.

قاب فناوری

تشخیص و درمان سریع «زردی» نوزادان

علیرضا احمدی/حدود ۶۰ درصد نوزادان در بدو تولد با بیماری زردی یا یرقان مواجه می‌شوند و در صورت بی‌توجهی به این بیماری و درمان نشدن نوزاد، امکان بروز مشکلات شنوایی یا صدمات مغزی وجود دارد. به‌همین دلیل هم تشخیص و درمان سریع زردی نوزادان از اهمیت بسیار زیادی برخوردار است. این، موضوعی است که فعالان عرصه فناوری به آن توجه کرده‌اند و با طراحی یک سیستم پیشرفته مبتنی بر تصویربرداری به‌کمک نوزادان مبتلا به زردی شتافته‌اند. این نوزادان به‌طور کلی به‌دلیل بالا بودن سطح یک پیگمنت زرد-نارنجی رنگ به‌نام بیلی روبین در جریان خون، دارای پوستی زردرنگ هستند. در مواردی که میزان این پیگمنت درحد خطرناکی بالا باشد، نور آبی رنگ به پوست نوزاد تابانده می‌شود تا بیلی روبین شکسته شود. پیش از این دستگاه‌های نوری مورد استفاده قرار می‌گرفت یا توسط یک مراقب به‌صورت دستی به پیشانی نوزاد می‌چسبید

تا با تجزیه و تحلیل رنگ پوست نوزاد، زردی وی تشخیص داده شده و درمان شود. اما حالا دانشمندان دانشگاه استرالیای جنوبی با همکاری دانشگاه Middle Technical عراق در جست‌وجوی جایگزینی تمام وقت و کمتر تهاجمی هستند. این محققان، سیستمی را توسعه داده‌اند که در آن یک وب‌کم معمولی ۱۰۸۰p به طور دائم و از فاصله ۳۰ سانتیمتری (۱۱.۸ اینچ) نوزاد را زیر نظر دارد. به‌منظور تجزیه و تحلیل مداوم خروجی دوربین هم یک ریزپردازنده متصل به‌نام Arduino Uno مورد استفاده قرارگرفته است که ازطریق یک برنامه سفارشی عمل می‌کند.

اگر نتایج تحلیل ریزپردازنده نشان دهد که پوست نوزاد، زردی بیش از حد دارد این پردازشگر به طور اتومات باعث می‌شود تا شدت نور چراغ LED افزایش یابد و به پوست کودک تابانده شود. به‌طور همزمان هم یک پیام هشداری برای پرستار و پزشک ارسال می‌شود. کل این فرایند تنها یک ثانیه طول می‌کشد که بسیار جالب توجه است. پزشک یا پرستار به محض دریافت پیامک بر بالین نوزاد حاضر می‌شود تا درصورت نیاز، میزان نور را کم یا زیادتر کند. درحال حاضر این سیستم برای تشخیص زردی و ارزیابی میزان بیلی روبین ۲۰ نوزاد مبتلا به یرقان مورد استفاده قرارگرفته و بسیار موفق بوده است.