

رویداد

اپلیکیشن برای پیشگیری ازمرگ باعکس سلفی

● **مهر:** گروهی از محققان تلاش می‌کنند تا اپلیکیشن مناسبی برای جلوگیری از وقوع حوادث دلخراش و حتی مرگ ناشی از گرفتن تصاویر سلفی ارائه کنند. براساس گزارش سی‌بی‌سی کانادا، تحقیقات نشان می‌دهد در فاصله سال‌های ۲۰۱۴ تا ۲۰۱۶ بالغ بر ۱۲۷ مرگ مرتبط با گرفتن عکس سلفی روی داده است. گروهی از محققان در دانشگاه کارنگی ملون با بررسی موقعیت‌های خطرناکی که افراد حین سلفی‌گرفتن در آنجا حاضر می‌شوند، طراحی و ساخت اپلیکیشنی را آغاز کرده‌اند که طور خودکار به افراد درباره قرار گرفتن در چنین موقعیت‌های خطرناکی هشدار می‌دهد. این اپلیکیشن که روی تلفن همراه نصب می‌شود با سنجش زوایای مختلف سطوح شیبدار و سایر فاکتورهای مرتبط با در معرض خطر قرارگرفتن سلامت افراد حاضر در عکس، هشدار لازم را منتشر می‌کند.

برنامه‌ریزی فیس‌بوک برای مقابله با اخبار جعلی

● **فارس:** هم‌زمان با تداوم انتقادات از فیس‌بوک به علت انتشار اخبار جعلی در این شبکه اجتماعی، مارک زاکربرج از برنامه‌های جدید خود برای مقابله با این مشکل خبر داد. براساس گزارش تک کرانچ، برخی کاربران پیروزی ترامپ در انتخابات ریاست‌جمهوری را ناشی از انتشار اخبار کذب در فیس‌بوک به نفع وی و به ضرر هیلاری کلینتون می‌دانند؛ امری که با تکذیب مارک زاکربرج مواجه شده است. او مدعی است کمتر از یک درصد از کل پست‌های فیس‌بوک را این نوع اخبار جعلی تشکیل می‌دهند، ولی برخی رسانه‌ها با انتشار مطالب متعددی دراین‌باره اغراق کرده‌اند. او در مطلبی که در این زمینه در فضای مجازی منتشر کرده، مدعی شده فیس‌بوک در زمینه برخورد با انتشار اخبار جعلی پیشرفت‌هایی داشته ولی باید کارهای بیشتری انجام دهد. زاکبرج افزود با سیستم‌های پیشرفته‌تر هوش مصنوعی که برای شناسایی اخبار دروغین استفاده خواهد شد، سیستم گزارش‌دهی این امر از سوی کاربران ساده‌تر می‌شود و در مورد این نوع مطالب پیام‌های هشداردهنده‌ای اضافه خواهند شد. فیس‌بوک همچنین هشدار داده سیاست‌های منتشرشده اخبار جعلی امکان استفاده و مشارکت در برنامه تبلیغاتی این شرکت را نخواهند داشت.

«ام‌اس‌آی» به سوددهی رسید

● **ایوروز:** آمار و ارقام ثبت‌شده در سه‌ماهه سوم سال جاری میلادی، خبر از سوددهی بسیار مناسب شرکت «ام‌اس‌آی» می‌دهند. براساس گزارش وب‌سایت خبری- تحلیلی Digitimes، شرکت میکرواستار اینترنشنال (ام‌اس‌آی) به‌تازگی آمار مالی جدید خود متعلق به سه‌ماهه سوم سال جاری میلادی را برای سهام‌داران و رسانه‌ها منتشر کرده است؛ این آمار نشان از آن داردن این شرکت آسیایی توانسته است تا در این مدت عملکرد خوبی در بازار از خود بر جای بگذارد و به واسطه آن نیز سود بسیار بالایی به دست بیاورد. مطابق اعداد و ارقام این شرکت، این پیشرفت به اندازه‌ای بالا بوده که در ابتدا ممکن است در درست درج‌شدن آمار مربوط به رشد درآمدی ام‌اس‌آی تردید داشته باشید، زیرا رشد ۷۲درصدی نسبت به سه‌ماهه دوم سال ۲۰۱۶، رقم معمولی و مرسومي در بازار به حساب نمی‌آید. همچنین در مقایسه درآمد این شرکت با ارقام پیش‌شده در پایان سه‌ماهه سوم سال ۲۰۱۵ نیز می‌توان رشدی ۴۱درصدی را مشاهده کرد که به‌خوبی روند رو به رشد این شرکت را نشان می‌دهد. گفتنی است میزان سود این شرکت نیز در مقایسه با سال گذشته میلادی به میزان ۲۰ درصد افزایش داشته، ولی در عملکرد ماهانه، میزان سود به‌دست‌آمده در ماه سپتامبر به نسبت میزان سود کسب‌شده در ماه اکتبر، کاهش پیدا کرده است.

پرتاب ۴هزار ماهواره برای ارائه خدمات جهانی اینترنت

● **مهر:** شرکت اسپیس‌ایکس متعلق به الون ماسک، سرمایه‌گذار بزرگ دنیای فناوری، قصد دارد برای ارائه خدمات اینترنت ماهواره‌ای فوق‌سریع بیش از چهار هزار ماهواره به فضا پرتاب کند. براساس گزارش یونیورسیتی هرال، تعداد دقیق ماهواره‌هایی که قرار است به فضا پرتاب شوند چهار هزار و ۴۲۵ ماهواره است. نکته جالب این است درحال‌حاضر تعداد کل ماهواره‌های فعال که به دور مدار زمین می‌چرخند هزار و ۴۱۹ مورد است و حالا فقط یک شرکت تجاری می‌خواهد تقریباً چهار برابر این تعداد ماهواره را به فضا پرتاب کند. درحال‌حاضر حدود دوهزار و ۶۰۰ ماهواره ازکارافشاده در فضا در حال گردش هستند و حتی با احتساب این رقم نیز شرکت اسپیس‌ایکس در حال ثبت رکوردی منحصربه‌فرد در زمینه پرتاب ماهواره به فضاست. هریک از این ماهواره‌ها می‌توانند منطقه‌ای به پهناي دوهزار و ۱۲۰ کیلومتر را پوشش دهند تا خدمات متشوع مخابراتی و اینترنتی در دسترس کاربران خانگی، تجاری و دولتی قرار گیرد. در مرحله اول این طرح، ۸۰۰ ماهواره به فضا پرتاب می‌شود و پس از بهینه‌سازی و تکمیل این طرح، پهنای باند اختصاص‌یافته به هر کاربر از این طریق به یک گیگابیت در ثانیه هم می‌رسد.

حدود ۲۵ تا ۳۰ میلیون گوشی هوشمند بدون گارانتی در دست خریداران تلفن همراه است و تعمیر این گوشی‌ها در زمان بروز مشکل، موضوعی است که در موارد متعدد مشکلاتی را برای مردم به همراه داشته است. آمار گوشی‌های هوشمند بدون گارانتی در حالی منتشر می‌شود که پیش‌تر عضو هیات عامل سازمان فناوری اطلاعات گفته بود: «از هر دو نفر حداقل یک نفر گوشی هوشمند در اختیار دارد که برآورد می‌شود شمار کاربران گوشی‌های هوشمند به ۴۰ میلیون نفر می‌رسد». او ادامه داده بود: «رسیدن آمار دو میلیون گوشی هوشمند در سال ۹۲ به ۲۰ میلیون گوشی در سال ۹۳ نشان‌دهنده فراهم‌شدن ابزار دولت موبایل است و رسیدن این عدد در سال ۹۴ به ۴۰ میلیون و از ابتدای سال ۹۵ تا به الان حدود ۵۰ میلیون گوشی هوشمند در کشور نشان از افزایش رو به رشد استفاده از گوشی همراه در کشور دارد. حال به نظر می‌رسد آمارهای ارائه‌شده از سوی مسئولان وزارت ارتباطات و فناوری اطلاعات، گویای آن است که ۴۰ میلیون گوشی تلفن همراه در کشور از مبادی غیرقانونی وارد می‌شود. بنابراین اگر میزان گوشی‌های قاچاق را از تعداد گوشی‌های اصلی تفکیک کنیم، حدود ۱۰ تا ۱۵ میلیون گوشی با گارانتی در کشور وجود دارد. البته علاوه بر گوشی‌هایی که ممکن است گارانتی آنها معتبر نباشد، گوشی‌های مختلفی نیز هستند که مدت گارانتی آنها به پایان رسیده، اگر به این فهرست گوشی‌های فاقد گارانتی را هم اضافه کنیم، مشخص می‌شود چندین میلیون گوشی در کشور وجود دارد که هنگام خرابی و بروز مشکل، پیداکردن تعمیرکاری مناسب برای آنها می‌تواند به یک معضل تبدیل شود. کارشناسان اتحادیه تجهیزات مخابراتی می‌گویند: «براساس تحقیقات صورت‌گرفته، اگر حتی

بحث قاچاق گوشی‌های موبایل برطرف شود حداقل در دو تا سه سال آینده در بازار گوشی‌های وجود دارد که نیاز به خدمات دارند. حال آنکه با توجه به آشفته بازار موجود لازم است سامانه‌هی خاصی دراین‌باره صورت گیرد تا تعمیرکاران خیابانی که فاقد تخصص و تجهیزات لازم هستند برای شهروندان مشکل ایجاد نکنند». مراجعه به تعمیرگاه‌های غیرمجاز در موارد مختلف برای مردم مشکلات متعدد ایجاد می‌کند برای مثال، ممکن است در مواردی قطعات غیراصلی برای تعمیر گوشی مورد استفاده قرار گرفته و برای آنها هزینه قطعه اصلی دریافت شود. گاهی نیز ممکن است هزینه‌های چندبرابری از مشتری دریافت شده و حتی دستگاه‌ها بدون تست کنترل کیفیت تحویل مشتری داده شده و پس از مدتی بسیار کوتاه دوباره دچار مشکل شوند. از سوی دیگر، در مواردی



هزینه تعویض قطعاتی مثل ال‌سی‌دی با قیمت‌هایی بالغ بر ۵۰۰ هزار تومان انجام می‌شود اما تعمیرکاران برای این قطعات هیچ گارانتی‌ای ارائه نکرده و این احتمال وجود دارد فرد پس از مدتی بار دیگر با هزینه بالا مجبور به تعمیرات مجدد شود. حتی گاهی بهتر آن است اصلا برای تعمیر یک گوشی هزینه‌ای صرف نشود، چراکه عمر مفید گوشی‌های هوشمند زمانی بین ۲۰۵ تا پنج سال است و پس از این مدت شاید تعمیر گوشی نیز فایده‌ای نداشته باشد. غلامحسین کریمی، رئیس اتحادیه تجهیزات مخابراتی، در گفت‌وگو با ایسنا، از لزوم طبقه‌بندی تعمیرکاران تلفن همراه خبر داد و این موضوع را از برنامه‌های آتی این اتحادیه دانست. او بیان کرد: «درباره گوشی‌هایی که دارای گارانتی هستند به طور طبیعی در مدت‌زمان گارانتی فرد نباید هزینه‌ای برای تعمیر گوشی خود

آزمایشگاه کسپر سکی پاسخ می‌دهد

چرا کاربران در شبکه‌های اجتماعی حبس می‌شوند

بررسی‌های اخیری که در بین چهارهزار و ۸۳۱ کاربر فعال شبکه‌های اجتماعی از سوی لابراتوار کسپرسکی انجام شد، نشان می‌دهد حدود ۷۸ درصد از پاسخ‌دهندگان به هر یک شبکه‌های اجتماعی خود فکر کرده‌اند، اما همچنان تصمیم به ماندن دارند. آنها دلایل مختلفی را برای ترک شبکه‌های اجتماعی داشتند: اما ۳۹ درصد کاربران از تلف‌شدن زمان زیاد خود شکایت کردند. بیشترین دلیلی که آنها را برای ماندن مصمم می‌کرد، تمایل تماس با بستگان و دوستان بود که پاسخ ۶۲ درصد از پاسخ‌دهندگان را شامل می‌شد. ۷۸ درصد از کاربران فعال شبکه‌های اجتماعی که در نظرسنجی شرکت کردند، در فکر ترک شبکه‌های اجتماعی خود بودند. دلایل کلیدی کاربران برای ترک شبکه‌های اجتماعی نشان می‌دهد ۱۰۳۹ درصد آنها از اتلاف وقت خسته می‌شوند و ۳۰ درصد آنها دوست نداشتند تحت نظارت غول‌های فناوری اطلاعات باشند. همچنین دلایل کلیدی که باعث می‌شود آنها نتوانند به‌راحتی شبکه‌های اجتماعی را کنار بگذارند، ارتباط با دوستان و خوشامداندنشان است که ۶۲ درصد را شامل می‌شود. ۲۸ درصد کاربران هم از ایده‌هایی که به‌عنوان راه‌حل برای کنترل بر لحظات دیجیتال آنها باشد، استقبال می‌کنند. سه ویژگی مهمی که در سرویس‌ها وجود دارد و پاسخ‌دهندگان به آنها اشاره کردند عبارت‌اند از: قابلیت محدودکردن دسترسی برای برنامه‌های سوم شخص (۵۰ درصد)، رمزنگاری قوی برای داده‌های ذخیره‌شده (۴۶ درصد)، ابزارهای ویژه برای تغییر تنظیمات اطلاعات ذخیره‌شده (۳۴ درصد). اولین سؤال این بود که «آیا شما تا به حال خواسته‌اید شبکه‌های اجتماعی را کنار بگذارید؟» در این سؤال ۷۸ درصد آنها خواستار این موضوع بودند. تعداد کمی از آنها (شش درصد) به‌ندرت از شبکه‌های اجتماعی استفاده دارند و اظهار تنفر کردند. حدود ۱۷ درصد آنها هرگز به ترک این شبکه‌ها فکر نکرده بودند. این نتایج با تمام کشورهای که ما آنها را بررسی کردیم،

بازار

تبلت‌های برتر برای اول آذرماه

اگر هدف اصلی شما وب‌گردی و تماشای فیلم‌هاست، تبلت می‌تواند تجربه بهتری را در مقایسه با گوشی هوشمند یا لپ‌تاپ و اولترا‌بوک برایتان فراهم کند و هنوز هم می‌توانید تبلت‌های خوبی در بازار پیدا کنید. از آنجا که موارد استفاده از تبلت بیشتر شامل وب‌گردی، تماشای فیلم و بازی می‌شود، صفحه‌نمایش را شاید بتوان مهم‌ترین عضو تبلت‌ها دانست.
Asus-zenpad-c-7-0
به گزارش فارنت، این تبلت محصولی ارزان‌قیمت و پایین‌رده محسوب می‌شود که با وجود این، از طراحی و چسبیت قابل‌قبولی در بازه قیمتی خود بهره می‌برد. توجه کنید در این رده قیمتی تبلت‌ها مناسب وب‌گردی سنگین یا بازی‌های گرافیکی نیستند. قیمت حدودی آن ۴۰۰ هزار تومان با گارانتی است.
galaxy-tab-a-2016
این تبلت گزینه دوم در بازه ارزان‌قیمت‌ها محسوب می‌شود که از صفحه‌نمایش، حافظه رم و پردازنده بهتری استفاده می‌کند و همچنین امکان اتصال به شبکه 4G را نیز دارد. قیمت حدودی آن ۵۴۰ هزار تومان بدون گارانتی (۷۰۰ هزار تومان با گارانتی) است.
asus-zenpad-8
این تبلت ارزان‌قیمت نسبت به گزینه قبلی از نسخه جدیدتر اندروید استفاده می‌کند، صفحه‌نمایش بزرگ‌تری داشته و حافظه داخلی و رم بیشتری هم در اختیار دارد. قیمت این محصول حدود ۶۳۰ هزار تومان با گارانتی است.
huawei-mediapad-m2-10
این تبلت را هم می‌توان یک میان‌رده خوب با کیفیت ساخت و امکانات مناسب دانست. اگر به تبلتی ۱۰اینچی احتیاج دارید این گزینه را در نظر بگیرید. در غیراین‌صورت گزینه قبلی به جز دوربین،

آمار ۵۰ میلیونی کاربران گوشی‌های تلفن هوشمند در ایران

۳۰ میلیون گوشی بدون گارانتی در دست مردم

پرداخت کند. البته در این زمینه شریایی نیز وجود دارد و برای مثال، اگر دستگاهی داخل آب افتاده یا ضربه خورده باشد، گارانتی آن ابطال می‌شود». او ادامه می‌دهد: «گاهی نیز ممکن است مدت‌زمان گارانتی به پایان رسیده باشد یا گوشی فاقد گارانتی باشد که در این موارد لازم است میان سرویس‌دهنده و سرویس‌گیرنده توافقات لازم پیش از انجام کار صورت گیرد. از سوی دیگر، ضروری است مردم از حقوق خود آگاه شوند تا بتوانند شرایط بهتری را تجربه کنند». او خطاب به مردم توصیه می‌کند پیش از انتخاب تعمیرگاهی برای تلفن همراه خود به برخی مسائل توجه کرده و مواردی مانند داشتن مجوز معتبر یا امکانات و تجهیزات مناسب را بررسی کنند، چراکه برای مثال، برای تعمیر گوشی‌های هوشمند لازم است فرد یک دستبند خاص داشته باشد تا آسی‌گوی گوشی باردار نشود در غیراین‌صورت ممکن است مشکلات متعددی برای تلفن‌همراه پیش آید. به گفته او، درحال‌حاضر در کشور بالغ بر ۵۰ میلیون گوشی هوشمند در دست مردم قرار دارد که هنگام تعمیر آنها لازم است افراد مجموعه‌ای معتبر را پیدا کنند. حال اگر ما در حوزه تعمیرات موبایل نیز دارای شرایطی شومیم که تعمیرگاه‌های دارای برند (نمانام) به فعالیت بپردازند، شاید این بازار ساماندهی شود، چراکه فعالیت شرکت‌های معتبر و برند می‌تواند در تأمین رضایت مشتری و کیفیت خدمات نقش بسزایی داشته باشد. حتی می‌توان به مرور زمان از این تعمیرگاه‌های برند برای ارائه خدمات به کشورهای همسایه نیز بهره گرفت. با وجود این، در شرایط موجود، همچنان مانند خرید موبایل در زمینه تعمیر نیز بازاری آشفته و نابسامان وجود دارد که گرانی‌های متعدد برای مردم ایجاد می‌کند.

وسایل خانگی همچون دوربین‌های مدرسته، ترموستات‌ها، دوربین‌های کنترل کودک، تلویزیون‌ها و یخچال‌ها، دارای آدرس IP اختصاصی خود می‌شوند و می‌توانند با کمک آن با یکدیگر و با سایر دستگاه‌ها ارتباط برقرار کنند. حجم ابزارآلات اینترنت اشیا که حتی درحال‌حاضر نیز بسیار گسترده است، انتظار می‌رود تا ۲۰۲۰ سه برابر شود و ۲۱ میلیارد دستگاه برسد. برای یک محافظ سایبری، این یعنی نه‌فقط هرک‌ها سه برابر بیشتر هدف برای حمله خواهند داشت، بلکه سه برابر بیشتر هم سیستم آسیب‌پذیر برای حمله به سایر دستگاه‌ها در دسترس آنها خواهد بود. این موضوع، چالش‌های جدیدی برای امنیت شبکه‌ها به وجود خواهد آورد و این تشخیص مسئول حملات را که درحال‌حاضر هم از نظر قانونی و عملی بسیار دشوار است، غبارآلودتر می‌کند.

مورد دومی که این تهدیدات را تقویت می‌کند همین‌گیربودن ابزارهای مورد استفاده برای انجام چنین حملاتی است. بدافزار جدید میرای (Mirai) که ماه گذشته برای ازکارآنداختن ۵۰ هزار دستگاه متصل به اینترنت استفاده شد، تهدید قدرتمندی است. باتنت (Botnet) یا درواقع گروهی از کامپیوترهای موردحمله واقع‌شده است که به ارثشی از زامبی-کامپیوترها برای حملات گسترده تبدیل شده‌اند و پدیده جدیدی نیست. چیزی که جدید است، تبدیل اینترنت اشیا به چنین ارثشی است. از طرفی، با توجه به نوع تهدیدات مستقل، سورس کد میرای، برخلاف سایر بدافزارهای سابق که به وسیله هرک‌های مورد حمایت دولت‌ها توسعه داده شده بودند، دیگر از سوی دولت‌ها و در کاوصندوق‌های اسناد محرمانه نگهداری نمی‌شود، بلکه در گوشه‌ونکار اینترنت و در تریک‌ترین فوروم‌ها بین هرک‌ها دست‌به‌دست می‌شوند و به هرکسی با هر نیتی به‌راحتی معامله می‌شود. این یعنی به‌زودی با سیلی از این بدافزارها مواجه خواهیم بود که هرکدام نسخه تغییریافته‌ای از میرای هستند و با فشار یک دکمه می‌توانند قسمتی از دنیای اینترنت را از کار بیاورند. این فرصت‌های خیلی دور از ذهن نیستند و موج انتقادات را علیه قابل‌اطمینان‌بودن اینترنت اشیا به ذهن متبادر می‌کنند. منتقدان سرسخت فناوری خواهند پرسید اصلا چرا باید یخچال من به اینترنت متصل باشد؟ اما این سؤال بجا نیست. درواقع به‌جای زیر سؤال‌بردن اینترنت اشیا باید به حل مشکل اصلی اندیشید، زیرا منافع متعدد اینترنت اشیا وجود آن را توجیه می‌کند. سؤال درست این است که چگونه از این حملات جلوگیری کنیم؟

اولین اقدام برای این منظور، وضع مقرراتی است که سطوح خاصی از امنیت سایبری را برای همه وسایلی که به اینترنت متصل می‌شوند، اجباری کند و اطمینان حاصل کنیم همه وسایل تا حد امکان امن هستند. این مورد تا حد زیادی قابل حصول است، زیرا خود سازندگان این محصولات نیز تمایل به امنیت آنها دارند. همچنین ما به فناوری‌های بهتری برای مدیریت آسیب‌پذیری‌های اینترنت اشیا به‌صورت لحظه‌ای و هم‌زمان نیاز داریم. همان‌گونه که شرکت‌های قابل‌اعتماد تولیدکننده فناوری، هنگامی‌که به نقطه‌ضعفی بی می‌برند، بسته‌های نرم‌افزاری جدید ارائه می‌دهند؛ تولیدکنندگان محصولات متصل به اینترنت اشیا نیز باید راهی برای آپدیت خودبه‌خود تجهیزات تولیدی خود قرار دهند و این نه‌فقط به عنوان یک بحث اختیاری، بلکه باید به عنوان یک مورد اجباری از اقدامات امنیتی موردنیاز قلمداد شود. همه ما مسئولیت خود را به عنوان خریداران و مصرف‌کنندگان نهایی اینترنت اشیا بشناسیم و قبول کنیم. ماه اکتبر در آمریکا، ماه هوشیاری امنیت سایبری بود و چقر بجا که بزرگ‌ترین حمله اینترنتی در این ماه رخ داد. حقیقت بنیادین درباره وضعیت دنیای مجازی و امنیت سایبری امروز ما این است که تقریباً «همه‌چیز» قابل هک شدن است. ۴۲۰ هزار تومان به فروش می‌رسد.

بازتاب

رایانه‌ها علیه انسان؛ دیگر رؤیانیست

اینترنت اشیا موجب شده است هر روز وسایل خانگی بیشتری به شبکه جهانی وب متصل شوند. چیزی که در نگاه اول، کمتر موردتوجه قرار می‌گیرد، این است که چکاری می‌توان انجام داد تا از ایمنی حرکت بعدی اینترنت مطمئن بود؟ به گزارش سایبربان، تا امروز، سهم بزرگی از حملات سایبری از سوی سازمان‌های نظامی، سرویس‌های اطلاعاتی خارجی یا سایر سازمان‌هایی که به وسیله دولت‌ها حمایت می‌شوند، سازماندهی می‌شدند که با اغراض سیاسی و جهت‌دهی‌های خاص، اقدام به حملات مختل‌کننده یا تخریب‌کننده برای دستیابی به اهداف مشخصی می‌کردند؛ اما رئیس اداره اطلاعات ملی آمریکا، جیمز کلپر (James Clapper)، می‌گوید حمله ماه اخیر، احتمالاً کارگروه‌های مرتبط با دولت‌ها نبوده است و این سخن او براساس گزارش‌های شرکت خصوصی امنیت سایبری فلش پوینت (Flashpoint)، قابل دفاع است. این بیانگر تحولی بزرگ و نمایانگر این است که موانع ورود به عرصه جرائم سایبری، آن‌قدر کوتاه شده که هرک‌های مستقل برای انجام خراب‌کاری، جرائم و حتی عملیات پیچیده سایبری، نیازی به حمایت و پشتیبانی حکومت‌ها ندارند. از دیگر چالش‌های به‌وجودآمده از حضور این بازیگران مستقل، به‌هم‌خوردن معادلات است، زیرا آنها دیگر تابع قوانین حکومت‌ها و روابط بین آنها نیستند، مرزهای جغرافیایی-سیاسی عمل می‌کنند و بنابراین ابزارهایی که پیش‌ازاین، برای جلوگیری از عملکرد خراب‌کارانه هرک‌های مورد حمایت استفاده می‌شد، دیگر کارایی ندارند.

وسایل خانگی همچون دوربین‌های مدرسته، ترموستات‌ها، دوربین‌های کنترل کودک، تلویزیون‌ها و یخچال‌ها، دارای آدرس IP اختصاصی خود می‌شوند و می‌توانند با کمک آن با یکدیگر و با سایر دستگاه‌ها ارتباط برقرار کنند. حجم ابزارآلات اینترنت اشیا که حتی درحال‌حاضر نیز بسیار گسترده است، انتظار می‌رود تا ۲۰۲۰ سه برابر شود و ۲۱ میلیارد دستگاه برسد. برای یک محافظ سایبری، این یعنی نه‌فقط هرک‌ها سه برابر بیشتر هدف برای حمله خواهند داشت، بلکه سه برابر بیشتر هم سیستم آسیب‌پذیر برای حمله به سایر دستگاه‌ها در دسترس آنها خواهد بود. این موضوع، چالش‌های جدیدی برای امنیت شبکه‌ها به وجود خواهد آورد و این تشخیص مسئول حملات را که درحال‌حاضر هم از نظر قانونی و عملی بسیار دشوار است، غبارآلودتر می‌کند.

مورد دومی که این تهدیدات را تقویت می‌کند همین‌گیربودن ابزارهای مورد استفاده برای انجام چنین حملاتی است. بدافزار جدید میرای (Mirai) که ماه گذشته برای ازکارآنداختن ۵۰ هزار دستگاه متصل به اینترنت استفاده شد، تهدید قدرتمندی است. باتنت (Botnet) یا درواقع گروهی از کامپیوترهای موردحمله واقع‌شده است که به ارثشی از زامبی-کامپیوترها برای حملات گسترده تبدیل شده‌اند و پدیده جدیدی نیست. چیزی که جدید است، تبدیل اینترنت اشیا به چنین ارثشی است. از طرفی، با توجه به نوع تهدیدات مستقل، سورس کد میرای، برخلاف سایر بدافزارهای سابق که به وسیله هرک‌های مورد حمایت دولت‌ها توسعه داده شده بودند، دیگر از سوی دولت‌ها و در کاوصندوق‌های اسناد محرمانه نگهداری نمی‌شود، بلکه در گوشه‌ونکار اینترنت و در تریک‌ترین فوروم‌ها بین هرک‌ها دست‌به‌دست می‌شوند و به هرکسی با هر نیتی به‌راحتی معامله می‌شود. این یعنی به‌زودی با سیلی از این بدافزارها مواجه خواهیم بود که هرکدام نسخه تغییریافته‌ای از میرای هستند و با فشار یک دکمه می‌توانند قسمتی از دنیای اینترنت را از کار بیاورند. این فرصت‌های خیلی دور از ذهن نیستند و موج انتقادات را علیه قابل‌اطمینان‌بودن اینترنت اشیا به ذهن متبادر می‌کنند. منتقدان سرسخت فناوری خواهند پرسید اصلا چرا باید یخچال من به اینترنت متصل باشد؟ اما این سؤال بجا نیست. درواقع به‌جای زیر سؤال‌بردن اینترنت اشیا باید به حل مشکل اصلی اندیشید، زیرا منافع متعدد اینترنت اشیا وجود آن را توجیه می‌کند. سؤال درست این است که چگونه از این حملات جلوگیری کنیم؟

اولین اقدام برای این منظور، وضع مقرراتی است که سطوح خاصی از امنیت سایبری را برای همه وسایلی که به اینترنت متصل می‌شوند، اجباری کند و اطمینان حاصل کنیم همه وسایل تا حد امکان امن هستند. این مورد تا حد زیادی قابل حصول است، زیرا خود سازندگان این محصولات نیز تمایل به امنیت آنها دارند. همچنین ما به فناوری‌های بهتری برای مدیریت آسیب‌پذیری‌های اینترنت اشیا به‌صورت لحظه‌ای و هم‌زمان نیاز داریم. همان‌گونه که شرکت‌های قابل‌اعتماد تولیدکننده فناوری، هنگامی‌که به نقطه‌ضعفی بی می‌برند، بسته‌های نرم‌افزاری جدید ارائه می‌دهند؛ تولیدکنندگان محصولات متصل به اینترنت اشیا نیز باید راهی برای آپدیت خودبه‌خود تجهیزات تولیدی خود قرار دهند و این نه‌فقط به عنوان یک بحث اختیاری، بلکه باید به عنوان یک مورد اجباری از اقدامات امنیتی موردنیاز قلمداد شود. همه ما مسئولیت خود را به عنوان خریداران و مصرف‌کنندگان نهایی اینترنت اشیا بشناسیم و قبول کنیم. ماه اکتبر در آمریکا، ماه هوشیاری امنیت سایبری بود و چقر بجا که بزرگ‌ترین حمله اینترنتی در این ماه رخ داد. حقیقت بنیادین درباره وضعیت دنیای مجازی و امنیت سایبری امروز ما این است که تقریباً «همه‌چیز» قابل هک شدن است.