مرکز تخصصی آپا
دانشگاه مازندران

نشریه مرکز آپا دانشگاه مازندران

شماره اول

اسفند ۹۷

۰۱۱-۳۵۳۰-۳۶۶۴

CERT.UMZ.AC.IR

CERT@UMZ.AC.IR

فهرست

گزارش عملکرد مرکز آپـا
در سال ۹۷

و

اولین دوره مسابقات ارزیابی
امنیتی اپلیکیشن های موبایل
در مازندران

آسیب پذیری ها

- آیا شرکت اپل رخنه داده را مخفی نگه داشته!؟
- مهم ترین رخنه های امنیتی سال۲۰۱۸
- وصله آسیب بحرانی مربوط به تصاویر png
- مبارزه توییتر با بات های سوء استفاده گر

آیا شرکت اپل در سال ۲۰۱۸ رخنه داده را مخفی نگه داشته است؟

گمانه‌زنی‌هایی وجود دارد مبنی بر اینکه اپل یک رخنه اطلاعاتی را در سال ۲۰۱۸ تجربه کرده و آن را از عموم مردم پنهان کرده است. به طورکلی این موضوع باعث شد تا شرکت‌ها تشویق شوند درباره رخنه‌های داده آگاه شوند و از این طریق کاربران درک کنند چه اتفاقی برای داده‌های آنها افتاده و متوجه شوند چه اقداماتی لازم است برای کاهش مشکل برداشته شود.

قوانین مربوط به اعلام رخنه‌ها بین کشورهای مختلف، متفاوت می‌باشد. مقررات حفاظت از اطلاعات عمومی اتحادیه اروپا دارای یک پنجره ۷۲ ساعته است که در آن شرکت باید تنظیم‌کنندگان آن مقررات را باخبر کند. اگر شرکت این کار را انجام ندهد، با مجازات شدیدی روبه‌رو خواهد شد.

اکنون ادعا شده است که اپل در اواخر سال گذشته یک رخنه داده را تجربه کرده است. یک محقق امنیتی با وب‌سایت خبری معروف در زمینه هک تماس گرفت تا نظرها را به نقص امنیتی که کشف کرده است، جلب کند. این نقص این امکان را به او می‌دهد تا برخی از داده‌ها را از حساب‌های تصادفی آی-کلود و کاربران هدف گذاری شده در آی-کلود با دانستن شماره تلفن آن‌ها مشاهده کند.

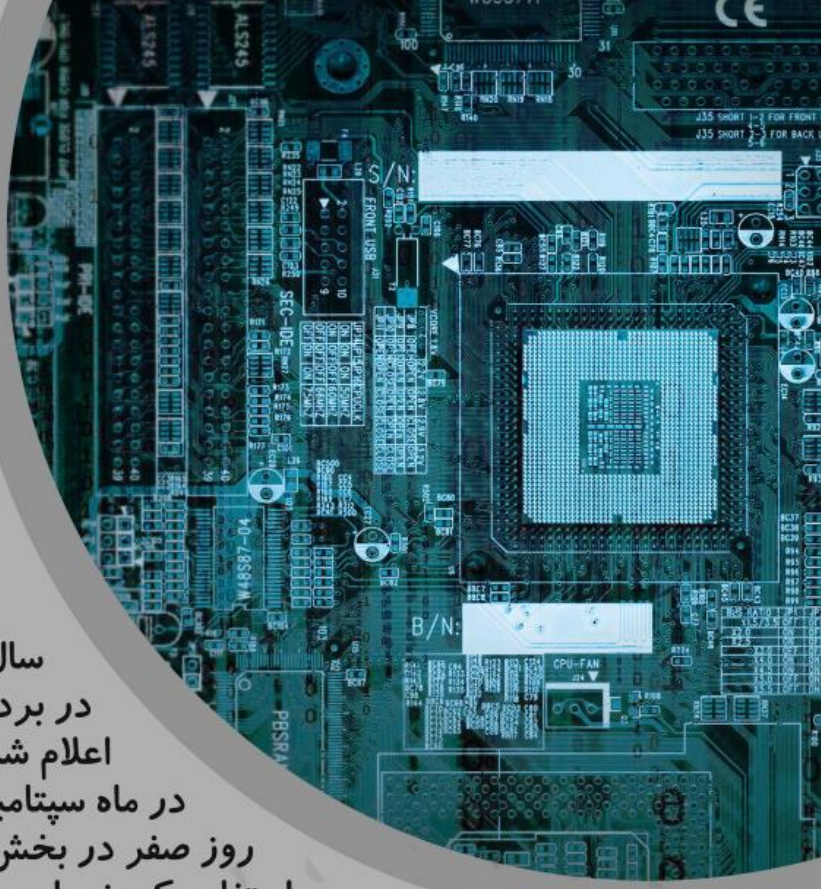
وی اظهار کرد:"من متوجه شدم که وقتی یک انتقال داده فعال بین کاربر و سرورهای اپل وجود دارد، اگر حساب کاربری آی-کلود مهاجم خود را باز کنم، امکان مشاهده برخی از داده‌های تصادفی در هر رفرش به دلیل این آسیب وجود دارد.

این محقق در اکتبر سال ۲۰۱۸ و مدت کوتاهی بعد از آن‌که این مسئله را کشف کرد، آن را به اپل گزارش داد. این نقص در نوامبر ۲۰۱۸ وصله شد. اپل به خبر منتشر شده توسط این محقق پاسخ داد و مدعی شد که پیش از این و قبل از دریافت جزئیات از وی، این موضوع را رفع کرده است.

این مسئله به این دلیل ایجاد شد که اپل به شیوه داخلی شماره تلفن ذخیره شده کاربر در اطلاعات صورتحساب خود را برای آی-کلود و یک دستگاه که از همان شماره استفاده می‌کند لینک کرد.

هنگامی که از اپل خواستند نظر خود را اعلام کند، به سادگی پاسخ داد که این مسئله در ماه نوامبر حل شده بود، اما آنها نمی‌دانستند که این نقص از کی وجود داشته و اینکه باورشان نمی‌شد که توسط مهاجمان مورد سوء استفاده قرار گرفته بودند.

منبع: yon.ir/vDoQo



مهم‌ترین رخنه‌های امنیتی سال ۲۰۱۸

سال ۲۰۱۸ رخنه‌های اطلاعاتی زیادی را در برداشت که این رخنه‌ها توسط شرکت‌ها اعلام شد.

در ماه سپتامبر زمانی که هکرها از آسیب‌پذیری روز صفر در بخش ویژگی "view as" فیس‌بوک سوء استفاده کردند، این شرکت بزرگترین رخنه داده را در طول تاریخ خود تجربه کرد که منجر به سرقت ۳۰ میلیون از نشانه‌های دسترسی شد.

- پایگاه داده شناسه دولت هند در ماه مارس هک شد. این پایگاه داده حاوی شناسه هر یک از شهروندان هند است و در برخی موارد نیز شامل مشخصات بیومتریک مانند اثرانگشت و اسکن عنبیه می‌باشد. این پایگاه داده،اطلاعات ۱.۱ میلیارد شهروند را در اختیار دارد.
- هتل‌های Marriott Starwood اعلام کردند که هکرها بین سال‌های ۲۰۱۴ و سپتامبر ۲۰۱۸، به پایگاه داده رزرواسیون که شامل سوابق ۵۰۰ میلیون مشتری بود، دسترسی داشته‌اند.
- نرم‌افزار MyFitnessPal در ماه مارس اعلام‌کرد که‌هکرها اطلاعات ۱۵۰ میلیون از کاربرانشان را به سرقت برده‌اند. این اطلاعات دزدیده شده شامل نام‌های کاربری، آدرس‌های ایمیل و کلمه‌های عبور رمزگذاری شده بود.
- وب‌گاه Quora اعلام کرد که هکرها اطلاعات ۱۰۰ میلیون کاربر، از جمله اسامی، آدرس‌های ایمیل، کلمه‌های عبور رمزگذاری شده و داده‌هایی از حسابهای مرتبط با این افراد را به سرقت بردند.
- گوگل پلاس اعلام کرد که به دلیل هک شدن داده‌های بیش از ۵۲.۵ میلیون کاربر خود، تصمیم به بستن رسانه اجتماعی خود دارد.

منبع: yon.ir/7rhO5

وصله آسیب بحرانی مربوط به تصاویر با پسوند .PNG توسط Google

گوگل یک آسیب‌پذیری بحرانی در نسخه‌های فعلی و قدیمی سیستم عامل اندروید خود را وصله کرده است که این آسیب‌پذیری این امکان را می‌دهد تا یک مهاجم فایل‌های تصویری با پسوند (PNG.) را به یک دستگاه هدفمند ارسال کند و کد دلخواه را اجرا نماید.

در بولتن امنیتی ماه فوریه مربوط به برنامه اندروید، گوگل سه مورد از آسیب‌پذیری‌های بحرانی اندروید را لیست کرده است. (CVE-۲۰۱۹-۱۹۸۷, CVE-۲۰۱۹-۱۹۸۶, CVE-۲۰۱۹-۱۹۸۸)یکی از آنها که به آسیب PNG مرتبط است، بر نسخه‌های سیستم عامل اندروید از نسخه (۷.۰) Nougat تا نسخه فعلی (۹.۰) Pie تاثیر گذاشته است.

طبق بولتن امنیتی"مهمترین این موارد، یک آسیب‌پذیری بحرانی امنیتی در چارچوب (اندروید) است که می‌تواند به یک مهاجم از راه دور این امکان را بدهد تا از یک فایل تصویری جعلی با پسوند PNG برای اجرای کد دلخواه در محدوده یک پردازه سطح بالا، استفاده کند."

مهاجمی که قصد سوء استفاده از این نقص را دارد می‌تواند از طریق ارسال یک تصویر تله موش، دستگاه اندروید آسیب‌پذیر را تحت کنترل بگیرد یا کاربر را فریب دهد تا لینک مخرب ارسال شده از طریق سرویس پیام تلفن همراه را دنبال کند. گوگل گفت که هیچ گزارشی وجود ندارد که در آن هیچ یک از آسیب‌پذیری‌های موجود در بولتن امنیتی ماه فوریه به این شدت مورد سوء استفاده قرار گرفته باشد.

این آسیب‌پذیری‌ها تنها سه مورد از ۱۱ آسیب بحرانی گزارش شده در روز دوشنبه به حساب می‌آیند. در مجموع، گوگل ۴۲ مورد را رفع کرد که ۳۰ مورد از این آسیب‌ها شدت بالایی داشتند. چهار مورد از این آسیب‌ها به اجزاء سخت‌افزاری اندروید که توسط NVIDIA ساخته شده بود و پنج مورد از این آسیب‌ها به تراشه‌ساز کوالکام مرتبط بودند.

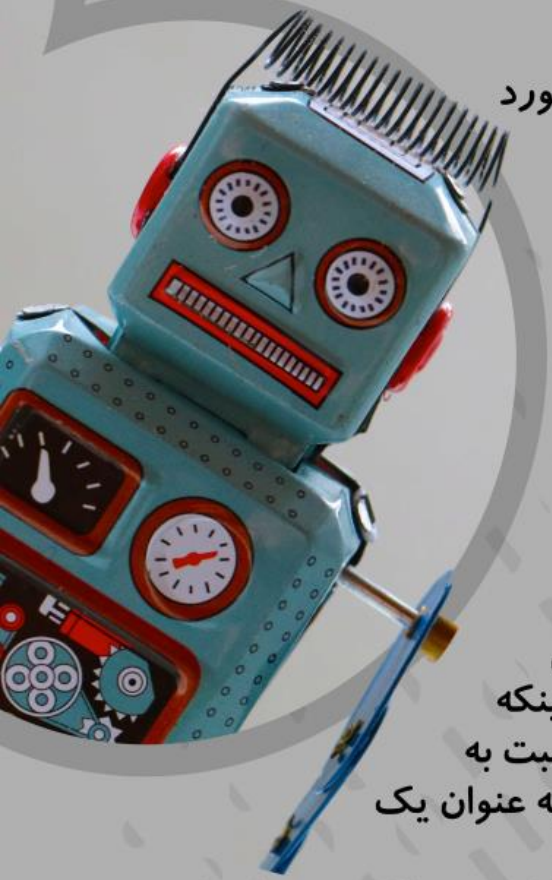
به‌روزرسانی‌هایی برای گوگل پیکسل و دیگر فروشندگان تلفن همراه (سامسونگ، ال جی و غیره) ظرف مدت ۴۸ ساعت از ارسال بولتن روز دوشنبه آغاز یا آماده خواهد شد. گوگل نوشت، "شرکای Android حداقل از یک ماه قبل از انتشار، از تمام مسائل مطلع شده بودند. وصله‌های کد منبع برای این مسائل در ۴۸ ساعت آینده برای مخزن پروژه متن‌باز اندروید منتشر خواهد شد."

انتظار می‌رود شرح مفصلی از CVEهای مربوط به بولتن امنیتی اندروید گوگل مربوط به ماه فوریه در روزهای آینده منتشر شود.شرکت ال جی شش آسیب‌پذیری بحرانی، همراه با ۲۱ آسیب سطح بالا و یک آسیب متوسط که بر گوشی‌های این شرکت تاثیر می‌گذارد را در روز دوشنبه وصله کرده است.

منبع: yon.ir/2CTdt

مبارزه مستمر توییتر
با بات های سوء استفاده کننده

در جریان انتخابات ریاست جمهوری سال ۲۰۱۶ امریکا، توییتر کمپین‌های اطلاعات غلط زیادی داشت که توسط بات‌ها یا حساب‌های جعلی اجرا می‌شد.



توییتر نسبت به بسیاری از پلت‌فرم‌های رسانه اجتماعی، بیشتر مورد هدف حساب‌های مجعول بود؛ اما چرا؟
توییتر بازترین پلت‌فرم رسانه اجتماعی است و این ویژگی آن رابرای هر کسی که مایل به اشتراک یک پیام است و مخاطبان زیادی دارد، جذاب می‌نماید. به عنوان نمونه می‌توان از سیاستمداران و روزنامه‌نگاران به‌عنوان کاربران بالقوه توییتر نام برد. با این حال، این باز بودن، توییتر را به یک مکان جذاب برای فعالیت هرزنامه تبدیل می‌کند.
توییتر می‌گوید بین ماه مه و ژوئن ۲۰۱۸، بیش از ۱۴۳،۰۰۰ برنامه را که به نوعی خط‌مشی‌های حریم خصوصی مربوط به آن را نقض کرده‌اند، حذف کرده است. واشنگتن پست همچنین گزارش داد که توییتر بیش از ۷۰ میلیون حساب جعلی در نیمه اول سال ۲۰۱۸ به حالت تعلیق درآورد. حتی با وجود اینکه توییتر سخت‌گیری خود را بیشتر کرده و موضع قویتری نسبت به حساب‌های مشکوک اتخاذ کرده است، اما این موضوع همچنان به عنوان یک مشکل عمده برای این پلت‌فرم به حساب می‌آید.
پروفسور زوبیر شفیق از دانشکده علوم کامپیوتر دانشگاه آیووا یک مطالعه ۱۶ ماهه از ۱.۵ میلیارد توئیت انجام داد. این مطالعه نشان داد که بیش از ۱۶۷،۰۰۰ برنامه از API توییتر برای تولید توییت روی حساب‌های جعلی استفاده کرده‌اند. همچنین مشخص شد که ۶۰٪ مواقع بیش از ۱۰۰ توییت از این حساب‌ها توییت شد قبل از آنکه توییتر آن‌ها را به عنوان حساب‌های سوء استفاده‌کننده شناسایی نماید.توییتر این ادعاها را انکار می‌کند و می‌گوید که این تحقیق، همه کارهایی که برای توقف توییت‌های سوء استفاده کننده انجام دادند را نشان نمی‌دهد؛ چرا که محققان تنها می‌توانند اطلاعات موجود در دسترس عموم را مشاهده کنند.

منبع: yon.ir/cvQOe


هشدار های امنیتی
آسیب‌پذیری‌هایی با درجه اهمیت بالا در Cisco RV۳۲۰/RV۳۲۵
هشدار امنیتی در خصوص افزایش شدید حملات بر بستر RDP

هشدار: آسیب‌پذیری‌هایی با درجه اهمیت بالا در Cisco RV۳۲۰/RV۳۲۵

تجهیزات Cisco Small Business RV۳۲۰ , RV۳۲۵ Dual Gigabit Wan VPN Router دارای دو آسیب‌پذیری با درجه اهمیت بالا هستند که یکی از آنها از نوع نشت اطلاعات حساس و دیگری از نوع تزریق دستور است. آسیب‌پذیری نشت اطلاعات حساس این آسیب‌پذیری با شناسه CVE-۲۰۱۹-۱۶۵۳ در رابط تحت وب تجهیزات مذکور نهفته است و به مهاجم احرازهویت نشده راه دور، اجازه استخراج اطلاعات حساس را می‌دهد. این آسیب‌پذیری ناشی از کنترل دسترسی نامناسب URL ها است. مهاجم می‌تواند بدین وسیله به اطلاعات پیکربندی یا اشکال‌زدایی (debug) تجهیز دست یابد.

آسیب‌پذیری تزریق دستو این آسیب‌پذیری که شناسه CVE-۲۰۱۹-۱۶۵۲ به آن اختصاص یافته است نیز ریشه در رابط تحت وب این تجهیزات دارد. منشاء آسیب‌پذیری، اعتبارسنجی نادرست ورودی کاربر است. مهاجم می‌تواند با ارسال درخواست مخرب POST از این نقص بهره‌برداری کند. با بهره‌برداری موفق می‌توان دستورات دلخواه را در قالب کاربر root روی shell لینوکس تجهیز اجرا کرد. بهره‌برداری از این آسیب پذیری نیازمند احراز هویت است.

کد بهره برداری از آسیب‌پذیری‌های فوق به طور عمومی منتشر شده است. همان طور که گفته شد، می‌توان با استفاده از آسیب‌پذیری اول، اطلاعات تجهیز از جمله اطلاعات کاربری درهم‌سازی (hash) شده را استخراج نمود. سپس می‌توان با شکستن hash ، اطلاعات کاربری را به دست آورده و از آسیب‌پذیری دوم بهره‌برداری نمود.

منبع: http://yon.ir/DefX4

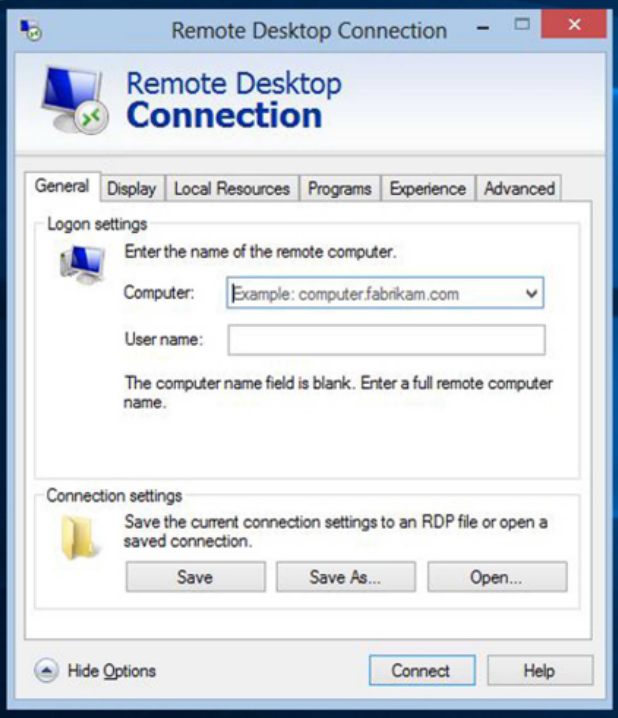
راه حل

مرکز ماهر اعلام کرد: سیسکو برای رفع آسیب‌پذیری‌های نامبرده، به‌روز رسانی‌هایی برای سخت‌افزار تجهیزات فوق منتشر کرده است. برای مصونیت از هر دو آسیب‌پذیری باید از نسخه ۱.۴.۲.۲۰ به بالا استفاده کرد.

هشدار امنیتی در خصوص
افزایش شدید حملات بر بستر RDP

بنابر گزارش شرکت امن پرداز (آنتی ویروس پادویش)، در روزهای گذشته شبکه‌های شرکت‌ها و سازمان‌های سراسر کشور، شاهد حجم بسیار بالایی از حملات هک و نفوذ به واسطه سرویس ریموت دسکتاپ و یا ابزارهای ریموت کلاینتی (مانند AnyDesk و ابزارهای مشابه) بوده‌اند. لذا توصیه همیشگی در مسدود سازی یا محدودسازی سرویس‌های مدیریتی دسترسی از راه دور از جمله RDP مجددا تکرار می‌گردد. ضروری است که از سوی مسئولین شبکه های سازمانها و شرکتها جهت جلوگیری از بروز اینگونه حملات اقداماتی پیشگیرانه نظیر تهیه پشتیبان به‌روز از اطلاعات حیاتی، غیرفعال کردن فوری دسترسی‌های مدیریتی راه دور و ... صورت پذیرد.

منبع: http://yon.ir/vEe6W



آخرین به‌روزرسانی ها

آخرین نسخه پایدار نرم‌افزارهای پرکاربرد

آخرین به‌روزرسانی‌های سیستم های عامل

آخرین نسخه پایدار نرم‌افزارهای پرکاربرد

موضوع	دسته بندی	آخرین نسخه‌ی پایدار	تاریخ عرضه	لینک دریافت
Apache Web Server	سرویس دهنده ها (وب، پست الکترونیک، پراکسی و غیره)	۲,۴,۳۸	۲۰۱۹-۰۱-۲۲	yon.ir/KdMym
Microsoft IIS	سرویس دهنده ها (وب، پست الکترونیک، پراکسی و غیره)	۱۰	۲۰۱۸-۱۰-۰۲	yon.ir/TuWhg
Squid Proxy & Cache Server	سرویس دهنده ها (وب، پست الکترونیک، پراکسی و غیره)	۴,۶	۲۰۱۹-۰۲-۱۹	yon.ir/GSeP۸
Php	زبان های برنامه نویسی	۷,۳.۳	۲۰۱۹-۰۳-۰۷	yon.ir/WzJDy
Python	زبان های برنامه نویسی	۳,۷,۲	۲۰۱۸-۱۲-۲۴	yon.ir/tWNrC
ASP.NET Core	زبان های برنامه نویسی	۳.۰	۲۰۱۹-۰۳-۰۶	yon.ir/FFAlQ
Joomla!	محیط های برنامه نویسی	۳,۹,۳	۲۰۱۹-۰۲-۱۲	yon.ir/۰BaQS
Drupal	محیط های برنامه نویسی	۸,۶,۱۰	۲۰۱۹-۰۲-۱۰	yon.ir/un۰SX
WordPress	محیط های برنامه نویسی	۵,۱	۲۰۱۹-۰۲-۲۱	yon.ir/T۰TQM
Mozilla Firefox	مرورگرهای اینترنت	۶۵,۰.۲	۲۰۱۹-۰۲-۲۸	yon.ir/I۸۱Fb
Google Chrome	مرورگرهای اینترنت	۷۲,۰,۳۶۲۶.۱۲۱	۲۰۱۹-۰۳-۰۴	yon.ir/t۴hBs

موضوع	دسته بندی	نسخه	تاریخ انتشار	لینک دریافت
Opera	مرورگرهای اینترنت	۵۸,۰,۳۱۳۵,۹۰	۲۰۱۹-۰۲-۰۷	yon.ir/FSo۴V
VMware ESXi	مجازی‌سازی	۶,۷,۰	۲۰۱۸-۱۰-۱۶	yon.ir/iFUJV
VMware Workstation	مجازی‌سازی	۱۵,۰,۲	۲۰۱۸-۱۱-۲۲	yon.ir/SymfT
VirtualBox	مجازیسازی	۶,۰,۴	۲۰۱۸-۰۱-۲۸	yon.ir/xC۱JK

آخرین به‌روزرسانی های سیستم های عامل

موضوع	دسته بندی	نسخه	لینک دریافت
Windows ۱۰	سیستم عامل	۱۸۰۹	yon.ir/aRDtM
Windows ۱۰	سیستم عامل	۱۸۰۳	yon.ir/B۰Jg۴
Windows ۸,۱	سیستم عامل	۹۶۰۰	yon.ir/۵YcAH
Windows ۸	سیستم عامل	۹۲۰۰	yon.ir/jIpPM
Windows ۷	سیستم عامل	۷۶۰۱	yon.ir/PIs۲L
Windows Server ۲۰۱۹	سیستم عامل	۱۷۷۶۱	yon.ir/RDuQd
Windows Server ۲۰۱۶	سیستم عامل	۱۷۱۳۴ (Version ۱۸۰۳)	yon.ir/aApoN
Windows Server ۲۰۱۲ R۲	سیستم عامل	۹۶۰۰	yon.ir/oN۴uu

آموزش

- امنیت کاربر رایانه
- تلفات بالقوه
- اصطلاحات ضروری
- ویژگی امنیت

امنیت کاربر رایانه

مرور دوران زیست بشر همواره می تواند موضوع شگفت انگیزی برای یادآوری باشد.ما با دسته بندی این دوران به اعصار مختلف مانند عصر حجر، عصر آتش ، عصر آهن ، عصر رنسانس و ... سعی کرده ایم موفقیت های پیشینیان در زمان های مختلف را راحت تر به خاطر بیاوریم و هر باربه این دستاوردها افتخار کنیم. اما مطمئنا اگر قرار باشد در آینده ای دور فرزندان نسل بشر، دورانی را که ما هم اکنون در آن روزگارمان را سپری می کنیم را به خاطر بیاورند ما را انسان های عصر کامپیوتر خواهند نامید.

پیشرفت روز افزون رایانه ها با به وجود آمدن رایانه های شخصی و تلفن های همراه هوشمند سرعت بیشتری گرفته است و اتصال به بستر اینترنت، همه این رایانه ها و موبایل ها را تبدیل به یک رایانه ی بسیار بزرگ در مقیاس جهانی کرده است که مالکیت آن متعلق به تمام کاربران رایانه در سراسر دنیاست. اما مساله ای که باید به آن توجه ویژه داشت این است که این استفاده شراکتی از بستر اینترنت می تواند چه خطراتی در زندگی روزمره ایجاد کند و ما به عنوان یک کاربر ، این رایانه ی جهانی برای حفظ امنیت و حریم شخصی خود و اطرافیانمان چه مواردی را باید مد نظر قرار دهیم؟

در همین رابطه در این بخش از این نشریه سعی شده است تا موارد امنیتی ضروری برای کاربران رایانه را با استفاده از مطالب مطرح شده در دوره ی "امنیت کاربر رایانه " با یکدیگر مرور کنیم.

در اولین قسمت از بخش " امنیت کاربر رایانه " به تعاریف و مفاهیم اولیه ی امنیت رخدادهای امنیتی و اصطلاحات ضروری امنیتی" خواهیم پرداخت.

تلفات بالقوه

اصطلاحات ضروری

آسیب پذیری

وجود یک خطای مربوط به ضعف طراحی یا پیاده سازی در سیستم که می تواند منجر به یک رویداد غیر منتظره و نامطلوب شده و امنیت سیستم را به خطر بیاندازد

اکسپلویت

یک شیوه ی تعریف شده برای نقض امنیت یک سیستم اطلاعاتی از طریق آسیب پذیری

تهدید

هر اقدام یا رویدادی که به صورت بالقوه توانایی نقض نمودن امنیت را دارد

سرقت داده

عمل ربودن اطلاعات از سیستم کاربر

حمله

هر اقدامی که برای نقض امنیت سیستم، از تهدیدهای هوشمندانه به وجود آمده است

کرَکر، مهاجم یا نفوذگر

فردی که به منظور سرقت اطلاعات، تغییر و یا تخریب آن ها وارد یک سیستم می گردد

ویژگی های امنیت

عدم انکار، بدین معنی است که طرف یک قرارداد یا یک ارتباط نتواند امضای خود را بر روی یک سند انکار نماید.

صحت، حصول اطمینان از دقیق بودن، کامل بودن، قابل اطمینان بودن و نیز اطمینان از این است که داده در فرم اصلی خود قرار دارد _ تغییر داده نشده است

محرمانگی، یعنی حصول اطمینان از اینکه اطلاعات تنها برای افراد مُجازی که حق دسترسی دارند قابل دسترس خواهد بود

(ISO-17799)

دسترس پذیری، یعنی حصول اطمینان از اینکه اطلاعات در صورت لزوم بدون تأخیر در دسترس افراد مجاز قرار می گیرد

اصالت، به معنای شناسایی و تضمین اصل بودن اطلاعات است

چک لیست امنیتی کامپیوتر

- استفاده از پسورد های قوی
- استفاده از آنتی ویروس ها
- بروزرسانی مداوم سیستم‌عامل ها و نرم افزارها
- پشتیبان گیری منظم از فایل های مهم
- استفاده از تکنیک های رمزنگاری و امضای دیجیتال
- استفاده از فایروال ها و سیستم های تشخیص نفوذ
- پیروی از دستورالعمل های استاندارد برای فعالیت های آنلاین
- امنیت فیزیکی زیرساخت های محاسباتی
- آگاهی از سناریوهای امنیتی و تکنیک های حمله

امنیت کودک و خانواده

- روانشناسی کودک و آسیب های فضای مجازی
- تعیین هویت دو عاملی چیست؟
- نرم افزار کتابراه
- معرفی اپلیکیشن های آموزش زبان

علائم هشداردهنده برای شناسایی آسیب‌های فضای مجازی بر کودکان

- اگر قبل و بعد از استفاده از اینترنت آشفته به نظر می‌رسند.
- رابطه او با ما، یا دیگر اعضای خانواده و دوستانش مختل شده است.
- وقت زیادی را در محیط های مجازی تا دیر وقت سپری می‌کند.
- اگر با تاریخچه خالی مرورگر روبرو شویم، یا با نزدیک شدن به رایانه از او عکس العمل نامربوط ببینیم
- بسته و تماس‌های تلفنی مشکوک دریافت کند.
- با بهانه آوردن‌های گوناگون از رفتن به مدرسه طفره رود.

راه حل:

- بیشتر تحقیق کنیم: اگر فکر می‌کنیم فرزندمان در معرض خطر جدی قرار گرفته از نرم افزارهای کنترلی استفاده کنیم.
- به بیان نکاتی درباره مشکلات دنیای مجازی بپردازیم.
- او را به صحبت کردن تشویق کنیم: بسیار مهم است که فرزندمان به چنین توضیحاتی با احتیاط پاسخ دهد.
- مسئله را بزرگ نکنیم: قبل از اینکه کاری انجام دهیم، ابتدا آرامش خود را حفظ کنیم.
- در مقابل رفتارهای ناامن او، عکس العمل مناسب داشته باشیم، طوری که آسیب ها را جبران کند و به فرزندمان بیاموزیم که در آینده انتخاب‌های درستی داشته باشد.
- اگر مدرکی مبنی بر سوءاستفاده افراد خطرناک از فرزندمان پیدا کردیم، با او برخورد نکنیم، با مشاوران آگاه تماس گرفته و تدابیر امنیتی بیندیشیم و در نهایت به پلیس مراجعه کنیم.
- فرزند خود را از مشارکت در مزاحمت‌های اینترنتی بر حذر داریم و بر اهمیت رفتار دوستانه در محیط های مجازی تاکید کنیم.

• اگر فرزندمان رفتاری خصمانه در محیط مجازی داشت، برای تغییر رفتار او پیشقدم شویم. مم-کن است خود ما مسئول آسیب ناشی از فرزندمان تلقی گردیم.

نکته: به فرزندان خود بیاموزید در صورت دریافت محتوای نامناسب، هرگز تلافی نکند. اما محتوای آسیب رسان را به عنوان مدرک نگه دارد و در تارنمای مربوطه طرح شکایت کند.

اگر این اقدامات موثر نبود، از ما کمک بخواهد. در اینصورت وظیفه ما این است که اگر فرد مزاحم را می‌شناسیم محتوای آسیب‌رسان را به والدینش نشان دهیم و خواستار توقف موضوع شویم، از مدرسه کمک بخواهیم و یا با پلیس فتا تماس بگیریم.

صحبتی دوستانه با فرزندان: ما والدین تو هستیم و لازم است از انتخاب‌های درست تو در محیط برخط آگاه باشیم. بنابراین به طور دوره‌ای سوابق فعالیت‌های تو و ارسال هایت در صفحات وب را بررسی خواهیم کرد. دیگران آنچه را که تو به صورت عمومی منتشر میکنی میبینند. اگر ببینیم که تو انتخاب‌های مناسبی داری، این کنترل را کم خواهیم کرد و در بیشتر موارد، قبل از بررسی موضوعی که نگران مان کرده، با خود تو، مشورت خواهیم کرد.

تعیین هویت دو عاملی

در دنیای رایانه همه چیز خیلی سریع حرکت می‌کند و اکنون دیگر دوره‌ی گذرواژه‌های ساده و معمول به پایان رسیده است. در دنیای اتصالات نامحدود هنوز ما در برخی موارد اساس امنیت خود را یک کد امنیتی قرار داده‌ایم؛ کدی که هر چه می‌گذرد نفوذ به آن آسان‌تر و محتمل‌تر می‌گردد.

با احراز هویت دومرحله‌ای شرکت‌های بزرگی چون گوگل، توییتر و فیس‌بوک سعی دارند معروف‌ترین تکنیک امنیتی شناخته شده در جهان را به قرن ۲۱ ببرند. در این نوشته مختصراً به توضیح احراز هویت دومرحله‌ای و چگونگی حفاظت بیش‌تر آن می‌پردازیم.

در ساده‌ترین بیان ممکن احراز هویت دو مرحله‌ای را می‌توان اقدام امنیتی اضافی دانست که در کنار سامانه‌ی گذرواژه‌ای موجود قرار می‌گیرد.

بدین معنا که در این روش هنوز هم نیاز
به نام کاربری و گذرواژه‌های سابق وجود دارد.
البته چنانچه بسیار هم توصیه شده توجه
داشته باشید که از گذرواژه‌های واضح و آسان
استفاده نکنید؛ چرا که ایناقدام بدترین اتفاق در دنیای امنیت است.
شکل دقیق این شیوه از احراز هویت در هر وب‌گاهی متفاوت است؛ اما اکثر سامانه‌ها پیام متنی را به شما ارسال می‌کنند که حاوی کد منحصربه‌فردی است و این کد در زمان ورود به سامانه در کنار نام کاربری و گذرواژه‌ی پیشین از شما درخواست می‌شود.
پیام‌های متنی محیط ایمنی برای ارسال کد فرض شده‌اند؛ چرا که اگر نفوذگر به گذرواژه‌ی شما نیز دسترسی یابد، احتمال اینکه تلفن‌همراه شما را نیز ربوده باشد، بسیار کم است. توجه داشته باشید که اگر شخصی تلفن همراه شما را به سرقت بُرد، باید هر چه سریع‌تر به تعویض گذرواژه‌ی خود اقدام کنید؛ حتی اگر از تکنیک احراز هویت دومرحله‌ای استفاده نمی کنید!

در اینده به توضیح این شیوه در ۳ وب‌گاه بزرگ گوگل، فیس‌بوک و توییتر می‌پردازیم تا دریابید این سامانه چگونه عمل می‌کند و چگونه می‌توانید آن را فعال کنید.

نرم افزار کتاب راه

یار "همیشه" مهربان

کودکان نسل جدید از جهتی باهوش هستند و از جهتی هم تن پرور. ما نباید نگاهی صفر و یک مطلق به تکنولوژی داشته باشیم؛ و اینکه کودکان را در دنیایی عاری از این وسایل بزرگ کرد هم غلط است،

ولی بعضا اعتیاد بیش از حدی هم وجود دارد که ناشی از همان درگیر بودن والدین بر سر کار و مسائل زندگی است. والدین بی‌حوصله شدند و ترجیح می‌دهند فرزندشان با یک وسیله بازی سرگرم شود تا اینکه تفریحات مختلفی برای او تدارک کنند. ضمن اینکه بقیه تفریح‌ها شاید گران هم باشد و وضعیت معیشت هم در این موضوع بی‌تاثیر نیست.

هرساله بسیاری از برنامه‌ها و بازی‌های اینترنتی منتشر می‌شود و نگرانی والدین را بر می انگیزد، اما همین والدین می‌توانند در این حوزه هم دست روی موارد درست و کاربردی بگذارند و این تهدید را تبدیل به فرصت کنند.برای مثال نرم افزارهای مختلفی مبنی بر رواج کتاب خوانی وجود دارد، مثل "کتاب راه" که یکی از برنامه های خوب در این زمینه است. شما می توانید مطابق سن و سلیقه فرزند خود کتاب مورد نظر را با هزینه ناچیز، دانلود کنید.

همچنین این نرم افزار شامل کتاب های صوتی نیز می باشد که جایگزین مناسبی برای موسیقی های نامناسب برای کودکان و نوجوانان است. این برنامه در رویدادهای مختلف، تخفیفاتی را برای کاربران خود در نظر می گیرد.

https://www.ketabrah.ir/landing

معرفی اپلیکیشن های آموزش زبان

با موفقیت اپلیکیشن های خارجی در سطح بین المللی، کم کم توسعه دهندگان داخلی هم به فکر ساخت نمونه های مشابه بومی افتادند و امروز ده ها اپلیکیشن خوب و باکیفیت آموزش زبان در فروشگاه های داخلی منتشر شده اند.در ادامه به سراغ تعدادی از این اپلیکیشن ها رفته ایم که تلاش دارند در سطوح مختلف و با شیوه های متفاوت، زبان انگلیسی را به شما آموزش بدهند. طبیعتا هر کدام از این اپلیکیشن ها مخاطب خاص خود را داشته و هر یک برای تقویت مهارت به خصوصی کوشش می کنند، ضمن این که بسته به امکانات در میزان حق اشتراک دریافتی هم تفاوت هایی با یکدیگر دارند.

آموزش زبان انگلیسی Learn it

ویژگی های برجسته: آموزش زبان از پایین ترین تا بالاترین سطح، رابط کاربری بسیار ساده و سر راست

لرنیت آموزش زبان را از نقطه صفر آغاز می کند، بنابراین برای افرادی که صرفا از انگلیسی با دایره محدودی از لغات آشنا هستند گزینه مناسبی به حساب می آید.

آموزش در لرنیت به شیوه کلاسیک انجام می گیرد: آشنایی با کلمات جدید، به کارگیری آن ها در مکالمه، آموزش گرامر، Speaking , Listening و در نهایت آزمون تستی؛ روشی که به عقیده بعضی مدرسین زبان هنوز هم کارآمد و موثر است.

آموزش زبان انگلیسی Expert

ویژگی های برجسته: یادگیری زبان با تماشای فیلم و گوش دادن آهنگ، آموزش از طـریق گوش دادن به داستان و کنفـرانس های واقـعی، جعبه لایتنراکسپرت برای آموزش دست روی روش بسـیار مؤثری گذاشته که شاید بسیاری از ما به طور غریزی زبان را به همین طریق یاد گرفته ایم: آموزش از طریق فیلم و سریال زیرنویس دار، آهنگ های خارجی، داستان و گوش دادن به کنفرانس ها و سخنرانی های واقعی.

البته متد آموزش چهار مهارت کلاسیک Reading, Listening , Speaking و Writing هم در این اپلیکیشن مشاهده می شود، بـنابراین با یک پکیج کامل مواجه هستید. اکسپرت لغات ضروری انـگلیـسی را با جعبه لایـتنر به شـما آمـوزش می دهد، و یک دیکـشـنری درون برنـامـه ای بسیـار عالـی هم دارد که با آن هـیچ اصـطلاحی در محـیط اپ برایتان نامفهوم باقی نخواهد ماند.

آموزش زبان انگلیسی Casco

کاسکو روی آموزش چهار مـهارت اصلی زبان و گرامر متـمرکز شده اما قابلیت هایی دارد که آن را به اپلیکیشن متمـایزی تبـدیل کرده اند. اولا بر خلاف اپ های دیگر این مطلـب، کاسکـو در کادر افقی به نمایـش در می آید که این موضـوع هم کار با اپ را آسـان تر کرده و هم باعث شده که فضای آن یادآور یک کتاب درسی باشد تا بهتر با آن ارتباط برقرار کنید.

یکی از قابلیت های خوب کاسکو، مکالمه هوشمند است که می تواند صدای شما و نحوه ادای کلمات را تشخیص بدهد. در این صورت برای تمـرین مکالمات این احسـاس به شما دست می دهد که دارید با یک پارتنر واقعی مکالمه را تمرین می کنید.

در نهایت باید بدانید که هـزینه آزادسـازی کلیه درس های کاسـکو ۱۰۰۰۰ تومان است.

گزارش عملکرد مرکز تخصصی آپا

در سال ۹۷

- ارزیابی امنیتی بیش از بیست سازمان و دستگاه اجرایی در سطح استان مازندران
- ارزیابی امنیتی اپلیکیشن‌های اندرویدی محبوب شرکت‌ها و نهادهای مطرح کشور
- رصد آسیب‌پذیری‌های امنیتی بیش از ده دانشگاه و موسسه آموزش عالی در سطح استان مازندران
- رصد آسیب‌پذیری‌های امنیتی پایگاه‌های اطلاع‌رسانی شوراهای اسلامی شهرهای استان مازندران
- رصد آسیب‌پذیری‌های امنیتی وب‌سایت برخی شخصیت‌های سیاسی کشور، شبکه‌های صدا و سیمای جمهوری اسلامی ایران، موتورهای جستجو ،...
- امدادرسانی به دستگاه‌های اجرایی استان در خصوص حوادث امنیتی نظیر آلودگی به باج‌افزار و ویروس
- تدوین و برگزاری دوره‌های مختلف آموزشی نظیر کارگاه تخصصی تست نفوذ و ارزیابی امنیتی، سمینار آشنایی با تکنیک‌های مهندسی اجتماعی، نشست علمی آشنایی با معماری اینترنت اشیاء، دوره امنیت کاربر رایانه
- حضور فعال در شبکه‌های اجتماعی و پیام‌رسان در جهت افزایش آگاهی آحاد جامعه در خصوص امنیت فضای مجازی
- ایجاد و مدیریت گروه مشاوره و هم‌اندیشی با مرکز آپا دانشگاه مازندران در شبکه اینترنتی کودک و خانواده
- تولید و انتشار مداوم اخبار و هشدارهای مهم مربوط به آسیب‌پذیری‌های فضای مجازی

مرکز تخصصی آپا
دانشگاه مازندران

مرکز تخصصی آپا دانشگاه مازندران برگزار میکند:

اولین دوره
مسابقات ارزیابی امنیتی
اپلیکیشن‌های موبایل در استان مازندران

MOBILE APPS SECURITY EVALUATION COMPETITION

براساس استاندارد های
MSTG , ASVA و MASVA
انجمن OWASP

ثبت نام در مسابقه در قالب
تیم‌های حداکثر سه نفره مجاز است

</همراه با جوایز نفیس و ارزنده>

جهت ثبت‌نام
به وبسایت مرکز آپا دانشگاه مازندران
مراجعه کنید
و یا با شماره تلفن زیر تماس حاصل نمایید.

۰۱۱-۳۵۳۰-۳۶۶۴

CERT.UMZ.AC.IR

CERT@UMZ.AC.IR

تاریخ ثبت نام:
تا پایان اسفند ۹۷

تاریخ برگزاری:
۲۵ الی ۳۱ فروردین ۹۸

دانشگاه مازندران
University of Mazandaran

مرکز ماهر
مرکز مدیریت امداد وهماهنگی عملیات رخداد های رایانه‌ای

همکاران این شماره :

میثم تقی پور
معصومه حسین‌زاده
سهیل سمن آبادی
هدی عباس زاده
محمد موفقی
غزال نوروزی

۰۱۱-۳۵۳۰-۳۶۶۴

CERT.UMZ.AC.IR

CERT@UMZ.AC.IR

T.ME/UMZ_CERT

APA_MAZANDARAN

مازندران - بابلسر -خیابان پاسداران

سازمان مرکزی