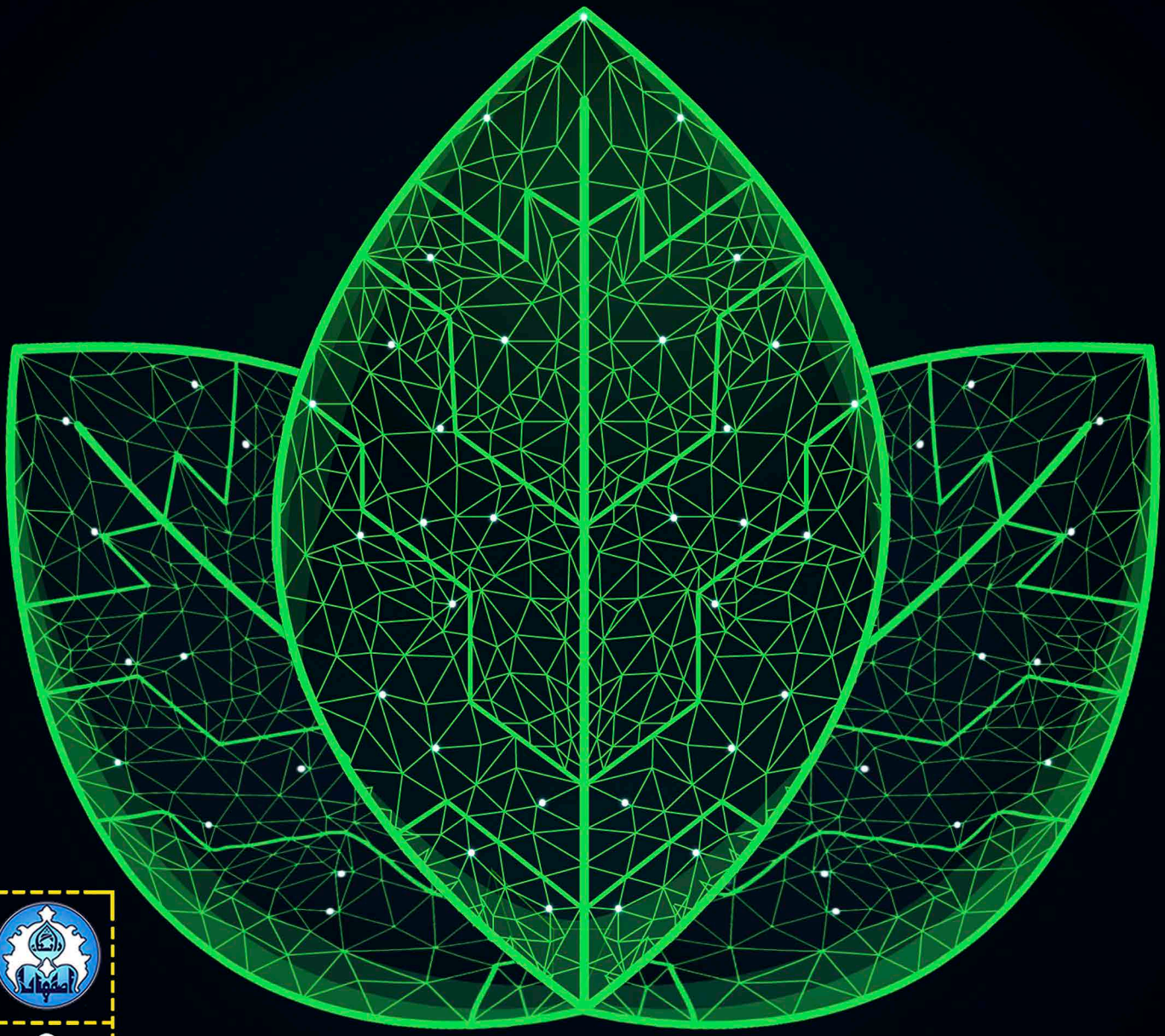
ماهنامه علمی

روز رمز

سال چهارم / شماره بیست‌وچهارم / فروردین‌ماه ۰۱



انجمن رمز ایران
iranian Society of Cryptology

این ماهنامه با حمایت مادی و معنوی اداره کل امور فرهنگی دانشگاه اصفهان چاپ و منتشر شده است.

نشریه علمی روز صفرم
شماره ۲۴ - فروردین ۱۴۰۱

صاحب امتیاز:
شاخه دانشجویی انجمن رمز ایران در دانشگاه اصفهان

سردبیر:
محمد آقائی

مدیر مسئول:
الهه رهبران

طراح جلد و صفحه‌آرا:
نوریه سادات مدنیان

هیئت تحریریه:
محمد آقائی
حسین علی ترکان
امیر فیض

اخبار:
سروش ذوالفقاری

ویراستار:
الهه رهبران

t.me/SBISC

SBISC.UI.AC.IR

t.me/CTFPREP

twitter.com/SBISC1

instagram.com/SBISC_UI

درباره انجمن:

شاخه دانشجویی انجمن رمز ایران در دانشگاه اصفهان از سال ۱۳۸۶ فعالیت خود را پیرامون مباحث مرتبط با امنیت اطلاعات آغاز کرد. این انجمن که هم‌اکنون یازده دوره از آغاز فعالیت آن می‌گذرد، تصمیم به انتشار نشریه‌ای با عنوان "**روز صفرم**" گرفته است تا از این طریق بتواند دانش امنیتی در فضای سایبر را به مخاطبان خود منتقل کند.این نشریه به صورت ماهانه و از اردیبهشت ۹۸ منتشر شده است.

ماه رمضان بر شما
مبارک باد.

مقایسه لینوکس و ویندوز در سرورها

Comparing Linux and Windows in Servers

محمد آقائی

mohammadaghaei800@gmail.com

سرور یک نرم‌افزار کامپیوتری یا ماشینی است که خدماتی را به برنامه‌ها یا دستگاه‌های دیگر ارائه می‌دهد که به آن‌ها «کلینت» گفته می‌شود. انواع مختلفی از سرورها وجود دارد: سرورهای وب، سرورهای پایگاه‌داده، سرورهای برنامه کاربردی، سرورهای محاسبات ابری، سرورهای فایل، سرورهای پست الکترونیکی، سرورهای DNS و موارد دیگر.

سهم استفاده از سیستم‌عامل‌های شبه یونیکس در طول سال‌ها، عمدتا در سرورها، با توزیع‌های لینوکس در خط مقدم، بسیار بهبود یافته است. امروزه درصد بیشتری از سرورهای اینترنت و مراکز داده در سراسر جهان از سیستم‌عامل مبتنی بر لینوکس استفاده می‌کنند. فقط برای درک بیشتر قدرت لینوکس در هدایت اینترنت، شرکت‌هایی مانند گوگل، فیس‌بوک، توییتر، آمازون و بسیاری دیگر، همه سرورهای خود را بر روی نرم‌افزار سرور مبتنی بر لینوکس اجرا می‌کنند. حتی قدرتمندترین ابرکامپیوتر جهان نیز بر روی یک سیستم‌عامل مبتنی بر لینوکس کار می‌کند.

عوامل متعددی در این امر نقش داشته است. در زیر، ما برخی از دلایل اصلی را توضیح داده‌ایم که چرا نرم‌افزار سرور لینوکس برای اجرای رایانه‌های سرور بهتر از ویندوز یا سایر پلتفرم‌ها است.

۱. رایگان و متن‌باز

لینوکس یا گنو/لینوکس رایگان و منبع باز است. می‌توانید کد منبع مورد استفاده برای ایجاد لینوکس (هسته) را مشاهده کنید. می‌توانید کد را بررسی کنید تا باگ‌ها را پیدا کنید، آسیب‌پذیری‌های امنیتی را بررسی کنید، یا به سادگی مطالعه کنید که آن کد روی دستگاه(های) شما چه می‌کند. علاوه‌بر این، به دلیل وجود رابط‌های برنامه‌نویسی متعددی که نیاز دارید، می‌توانید به راحتی برنامه‌های خود را در یک سیستم‌عامل لینوکس توسعه و نصب کنید. با تمام ویژگی‌های فوق، می‌توانید یک سیستم‌عامل لینوکس را در ابتدایی‌ترین سطوح آن متناسب با نیازهای سرور خود بر خلاف ویندوز تنظیم کنید.

۲. ثبات و قابلیت اطمینان

لینوکس مبتنی بر یونیکس است و یونیکس در ابتدا برای ارائه محیطی قدرتمند، پایدار و قابل اعتماد و در عین حال آسان برای استفاده طراحی شده بود. سیستم‌های لینوکس به دلیل پایداری و قابلیت اطمینان، خود به طور گسترده‌ای شناخته شده‌اند، بسیاری از سرورهای لینوکس در اینترنت، سال‌ها بدون خرابی یا حتی راه‌اندازی مجدد کار می‌کنند.. سوال این است که درواقع چه چیزی سیستم‌های لینوکس را پایدار می‌کند. عوامل تعیین‌کننده زیادی وجود دارد که شامل مدیریت تنظیمات سیستم و برنامه‌ها، مدیریت فرایند، اجرای امنیت و غیره می‌شود. در لینوکس، می‌توانید فایل پیکربندی سیستم یا برنامه را تغییر دهید و تغییرات را بدون نیاز به راه‌اندازی مجدد

سرور اعمال کنید، که در مورد ویندوز صدق نمی‌کند. همچنین مکانیزم‌های کارآمد و قابل اعتماد مدیریت فرایند را ارائه می‌دهد. درصورتی که فرایندی غیرعادی رفتار کند، می‌توانید با استفاده از دستوراتی مانند pkill، kill و killall سیگنال مناسبی برای آن ارسال کنید.
لینوکس همچنین امن است، نفوذ منابع خارجی (کاربران، برنامه‌ها یا سیستم‌ها) را که احتمالا می‌توانند سرور را بی‌ثبات کنند، بسیار محدود می‌کند.

۳. امنیت

لینوکس بدون شک ایمن‌ترین هسته موجود است که سیستم‌عامل‌های مبتنی بر لینوکس را امن و مناسب برای سرورها می‌کند. برای مفید بودن، سرور باید بتواند درخواست‌های سرویس‌های مشتریان راه دور را بپذیرد و سرور با اجازه دادن برخی از دسترسی‌ها به پورت‌های خود همیشه آسیب‌پذیر است.
با این حال، لینوکس مکانیسم‌های امنیتی مختلفی را برای ایمن‌سازی فایل‌ها و سرویس‌ها در برابر حملات و سوءاستفاده‌ها پیاده‌سازی می‌کند. می‌توانید با استفاده از برنامه‌هایی مانند فایروال (مثلا iptables)، پوشش‌های TCP (برای اجازه دادن و ممانعت از دسترسی به سرویس) و لینوکس تقویت‌شده امنیت (SELinux) که به محدود کردن منابعی که یک سرویس می‌تواند به آن دسترسی داشته باشد، ایمن کنید. SELinux تضمین می‌کند که سرور HTTP، سرور FTP، سرور Samba یا سرور DNS می‌تواند تنها به مجموعه‌ای از فایل‌های محدود شده روی سیستم که توسط زمینه‌های فایل تعریف شده است دسترسی داشته باشد و تنها به مجموعه‌ای از ویژگی‌های محدودی که توسط Booleans تعریف شده است اجازه دهد.
تعدادی از توزیع‌های لینوکس مانند فدورا، RHEL/CentOS و تعدادی دیگر با ویژگی SELinux عرضه می‌شوند و به‌طور پیش‌فرض فعال می‌شوند. با این حال، در صورت نیاز، می‌توانید SELinux را به طور موقت یا دائم غیرفعال کنید.
در مجموع، در لینوکس، قبل از این‌که هر کاربر/گروه یا برنامه سیستمی به منبعی دسترسی پیدا کند یا یک فایل/برنامه را اجرا کند، باید مجوزهای مناسب را داشته باشد، در غیر این صورت هر گونه اقدام غیرمجاز همیشه مسدود می‌شود.

۴. انعطاف‌پذیری

لینوکس بسیار قدرتمند و انعطاف‌پذیر است. می‌توانید آن را طوری تنظیم کنید که نیازهای سرور شما را برآورده کند: به شما امکان می‌دهد هر کاری را که می‌خواهید انجام دهید (در صورت امکان). شما می‌توانید یک رابط کاربری گرافیکی نصب کنید یا به سادگی سرور خود را فقط از طریق ترمینال اداره کنید.
هزاران ابزار را ارائه می‌دهد که می‌توانید برای انجام کارهایی مانند راه‌اندازی سیستم و مدیریت خدمات، افزودن کاربران، مدیریت شبکه و دیسک‌ها، نصب نرم‌افزار، نظارت بر عملکرد و به طور کلی ایمن و مدیریت سرور خود را انتخاب کنید. همچنین به شما امکان می‌دهد فایل‌های باینری را نصب کنید یا از کد منبع برنامه بسازید.
یکی از قوی‌ترین برنامه‌های استاندارد موجود در لینوکس، پوسته (theme) است، برنامه‌ای است که محیطی سازگار برای اجرای برنامه‌های دیگر در لینوکس در اختیار شما قرار می‌دهد. این به شما کمک می‌کند تا با خود هسته یا کرنل تعامل داشته باشید.
نکته مهم این است که پوسته لینوکس ساختارهای برنامه نویسی عملی را ارائه می‌دهد که به شما امکان می‌دهد تصمیم بگیرید، دستورات را به طور مکرر اجرا کنید، عملکردها/ابزارهای جدید ایجاد کنید و وظایف مدیریت روزانه سرور خودکار را انجام دهید.
اساسا، لینوکس به شما کنترل مطلق روی یک ماشین می‌دهد و به شما کمک می‌کند تا سروری را همان‌طور که می‌خواهید بسازید و سفارشی کنید.

۵. پشتیبانی سخت‌افزاری

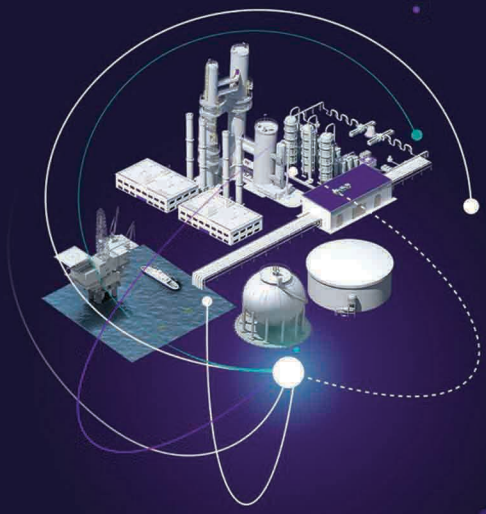
لینوکس از ترکیبی از معماری‌های کامپیوتری، چه بر روی سخت‌افزار مدرن و چه نسبتا قدیمی، پشتیبانی قوی دارد. این یکی از مهمترین عواملی است که لینوکس را نسبت به ویندوز برای سرورها بهتر می‌کند، خصوصا اگر بودجه کمی برای خرید سخت‌افزار دارید.
لینوکس به طور قابل توجهی از سخت‌افزار نسبتا قدیمی پشتیبانی می‌کند، برای مثال سایت Slackware Linux بر روی پنتیوم III، ۶۰۰ مگاهرتز، با ۵۱۲ مگابایت رم میزبانی می‌شود. می‌توانید لیست سخت‌افزارهای پشتیبانی شده و الزامات مربوط به یک توزیع خاص را از وب‌سایت‌های رسمی آن‌ها بیابید.

۶. هزینه کل مالکیت (TCO) و نگهداری

در نهایت، هزینه کل داشتن و نگهداری یک سرور لینوکس در مقایسه با سرور ویندوز، از نظر هزینه‌های مجوز، هزینه‌های خرید و نگهداری نرم‌افزار/سخت‌افزار، خدمات پشتیبانی سیستم و هزینه‌های اداری کمتر است.
مگر این‌که از توزیع اختصاصی لینوکس مانند سرور لینوکس RHEL یا SUSE استفاده کنید که نیاز به اشتراک داشته باشد، برای این‌که بتوانید پشتیبانی و خدمات ممتاز را دریافت کنید، هنگام اجرای سرور لینوکس با هزینه‌های مقرون‌به‌صرفه‌ای روبه‌رو خواهید شد.
مطالعات انجام شده توسط گروه رابرت فرانسیس (RFG) و شرکت‌های مشابه، در گذشته اخیر نشان داده است که لینوکس در یک محیط سرور معمولی قابل مقایسه با ویندوز یا سولاریس، به ویژه برای استقرار وب، ارزان‌تر است.

در نتیجه
لینوکس امروزه به یک پلتفرم استراتژیک، کارآمد و قابل اعتماد برای سیستم‌های تجاری در بسیاری از شرکت‌های کوچک، متوسط و بزرگ تبدیل شده است. درصد بیشتری از سرورهای تغذیه‌کننده اینترنت بر روی یک سیستم‌عامل مبتنی بر لینوکس اجرا می‌شوند و این به دلایل کلیدی بالا نسبت داده شده است.

منابع:
• why linux is better than windows for servers ,tecmint.com
• project zero finds that linux developers fix security flaws faster than apple google or microsoft, betanews.com



امنیت سایبری در نیروگاه‌ها

Cyber Security in Power Plants

حسین علی ترکان

h.alitorkan1380@gmail.com

نیروگاه‌ها از مهم‌ترین و حیاتی‌ترین اجزای زیرساخت تمدن مدرن به حساب می‌آیند. اختلال در عملکرد آن‌ها می‌تواند بر ساختار همه اجزای جامعه از امنیت ملی تا مراکز درمانی تاثیر داشته باشد و از بین بردن توان تولید انرژی یک کشور هدف خوبی برای دشمنان است. از این رو نیازمند اقدامات موثر دفاعی است. با این‌که هنوز امکان حمله فیزیکی به یک نیروگاه وجود دارد، اما امروزه بسیاری از تهدیداتی که مراکز حساس با آن روبه‌رو هستند از نوع سایبری است و نیروگاه‌ها هدف بسیار جذابی برای هکران به حساب می‌آیند. از این رو شبکه‌های نیروگاهی در ۲۴ ساعت شبانه روز و در تمام طول سال مورد حمله هکرهای مختلف قرار می‌گیرند. هدف آن‌ها این است که با عبور از موانع و سپرها مانند فایروال‌های خارجی به شبکه‌های داخلی دسترسی پیدا کنند و کنترل را در دست بگیرند و مقاصد خراب‌کارانه خود را دنبال کنند. هکرها معمولاً از اسکنر پورت، نرم‌افزار حدس رمز عبور و سایر ابزارهای در دسترس برای انجام حملات بی‌وقفه علیه محیط‌های نیروگاه استفاده می‌کنند. این ابزارها هر گونه ضعف بالقوه‌ای را که می‌تواند برای دسترسی به شبکه‌های داخلی مورد استفاده قرار گیرد، جست‌وجو کرده و از آن‌ها بهره‌برداری می‌کنند.

چرا نیروگاه‌ها در برابرحملات آسیب‌پذیر هستند؟

• در گذشته شبکه‌های فناوری اطلاعات (IT) و فناوری‌های عملیاتی و اجرایی (OT) ارتباط مستقیم چندانی نداشتند و تکنسین‌ها و اپراتورها برای مدیریت سیستم‌های کنترل باید به صورت فیزیکی در محل مورد نظر حاضر می‌شدند ولی امروزه پیشرفت‌ها در اتوماسیون و اتوماتیک‌سازی منجر به ادغام سیستم‌ها و تغییر آن‌ها به سیستم‌های دیجیتالی کنترل‌شونده از راه دور شده است و این مورد با وجود ایجاد بهبود در برخی زمینه‌ها، خطرات و نقاط ضعف جدیدی در سیستم به وجود می‌آورد و به دنبال آن برای عوامل مخرب راه‌های جدیدی را به وجود می‌آورد تا سیستم‌های عملیاتی که در تولید برق استفاده می‌شوند را به خطر انداخته و دچار اختلال کنند.

• احراز هویت ضعیف و نفوذ از طریق واسطه‌ها: هکرها همیشه دنبال سیستم‌هایی با احراز هویت ضعیف هستند. حساب‌ها با رمز عبور ضعیف یا پیش‌فرض می‌توانند دروازه‌ای برای ورود عوامل مخرب باشند. علاوه بر این می‌توان با مهندسی اجتماعی و نفوذ در کادر انسانی یا شرکت‌های زیرمجموعه و آلوده کردن آن‌ها به بدافزارها، به سیستم‌های مورد نظر نفوذ کرد. مانند ویروس استاکس‌نت که گفته می‌شود از طریق یک فلش مموری به تاسیسات هسته‌ای منتقل شده بود، در حالی که این تاسیسات به دلیل حساسیت بالا به شبکه جهانی اینترنت متصل نبود. این موارد در مورد بقیه مراکز حساس مانند نیروگاه نیز می‌تواند صادق باشد.

• افزایش تعداد افراد لاگین در سیستم: به دلیل افزایش IOT و نیاز به دسترسی از راه دور و افزایش دورکاری به خاطر کرونا، نقاط دسترسی و لاگین به سیستم افزایش یافته است، که این امر سیستم را در معرض خطر بیشتری قرار می دهد زیرا هر نقطه دسترسی می تواند راهی برای نفوذ هکرها باشد.

تهدید حملات سایبری را باید جدی گرفت. امروزه تهدیدات سایبری بسیار مهم هستند و عدم توجه به آن‌ها می‌تواند مشکلات زیادی را ایجاد کند، همان‌طور که مثال‌هایی از هک شدن مراکز کشورهای مختلف توسط دشمنانشان وجود دارد. حملات به شبکه برق اوکراین در سال‌های ۲۰۱۵ و ۲۰۱۶ یکی از فاجعه‌بارترین حملات به تاسیسات تولید نیرو است. این اولین مورد تایید شده از قطع شبکه برق توسط هکرها است که منجر به بدون برق رها شدن صدها هزار شهروند شد. این مورد خود باعث ایجاد خسارات و هزینه‌های زیادی می‌شود. برق در عرض چند ساعت به اکثر مشتریان بازگردانده شد، اما هکرها سیستم‌عامل را بازنویسی کردند و کار تکنسین‌ها را برای کنترل تجهیزات خود از راه دور غیرممکن کردند بودند.
برای مثالی دیگر در حادثه Solar winds که هکرهای روسی مسئول آن شناخته می‌شوند، هزاران کاربر تحت تاثیر قرار گرفتند و هنوز به طور کامل ابعاد آن شناخته نشده است. در این مورد هکرها به‌روزرسانی سیستم محبوب نظارتی و مانیتوریگ را همراه با بدافزار منتشر کردند. این مورد باعث شد تا بسیاری از کاربران آن را دانلود کرده و حفره امنیتی در طیف گسترده‌ای از سیستم‌ها ایجاد شود. تقریبا ۲۵ درصد از شرکت‌های شبکه برق آمریکای شمالی آن را دانلود کرده بودند.
قسمت مخوف‌تر داستان این‌جاست که هکرها گاهی بدافزارهای مخفی با اهداف بلندمدت ایجاد می‌کنند تا در موقعیت مناسب از آن استفاده کنند و تا سال‌ها ممکن است فعالیتی نداشته باشند و یا محاسبه خسارت آن‌ها ممکن نباشد و مخفی بماند. بسیاری از محصولات نرم افزاری در حال استفاده نیز می‌توانند به طور مشابه آلوده به این بدافزارها باشند.

محافظت از نیروگاه‌ها و رسیدگی فعالانه اسیب‌پذیرها

برای محافظت از نیروگاه نیاز به چندین لایه امنیتی است و باید به طور مستمر مورد بررسی قرار گیرد. از جمله مواردی که برای افزایش امنیت نیروگاه‌ها انجام می‌دهند می‌توان به موارد زیر اشاره کرد:
• بهبود احراز هویت‌ها با استفاده از شیوه‌های درست مانند احراز هویت دو مرحله‌ای و ملزم کردن استفاده از رمزهای مناسب و پیچیده و کوتاه کردن مدت زمان انقضای توکن‌ها و رمزها و کاهش نقاط و سطح دسترسی در حد امکان.

• افزایش تست‌های امنیتی مختلف شامل تست نفوذ و امنیت فیزیکی برای شناسایی مناطقی که باید بیشتر امن شوند ضروری است.

• کاربران در سراسر سازمان باید در مورد خطرات مرتبط با ایمیل‌های فیشینگ یا سایر کمپین‌های طراحی شده برای فریب دادن آن‌ها، در کنار گذاشتن اعتبار ورود یا انتشار ناخواسته بدافزار، آموزش ببینند و کادر مناسب از لحاظ پیشینه امنیتی برای موقعیت‌های حساس فراهم شود تا از سواستفاده توسط سازمان‌های جاسوسی و نظامی کشورهای دیگر و بقیه گروه‌ها در امان باشد. بر اساس برخی اطلاعات منتشر شده فیلم‌های تبلیغاتی از مرکز هسته‌ای و عوامل نفوذی، اطلاعات خوبی به سازمان‌های جاسوسی برای ایجاد ویروس استاکس‌نت داده است که این موارد باید در همه مراکز حساس در نظر گرفته شوند.

• پچ‌های امنیتی باید به سرعت آزمایش و پیاده‌سازی شوند تا زمان در دسترس هکرها برای بهره‌برداری از آسیب‌پذیری‌های شناسایی شده به حداقل برسد.

منبع:
• power plants security threats, helpnetsecurity.com

اسب تروجان

Trojan Horse

امیر فیض

amir.feiz.1381@gmail.com

در زندگی روزمره بسیاری از اسم‌هایی که در موارد مختلف استفاده می‌کنیم برگرفته از مسائل تاریخی هستند و امنیت هم از این موضوع مستثنی نیست. یکی از زیباترین و مرموزترین انواع نفوذ، اسب تروجان است که در بسیاری از فیلم‌ها و مستندها استفاده شده و به احتمال زیاد نام و روش آن را شنیده‌اید. در این مقاله قرار است بیشتر به این روش نفوذ بپردازیم.

در مرحله اول باید به دقت به داستان تاریخی اسب تروآ یا تروجان بپردازیم. در عصر برنز شهری به نام تروآ وجود داشت. طبق افسانه‌ها یکی از خدایان به نام پوزئیدون به کمک فرزند زئوس، آپولون، یک حصار قوی و بزرگ و تقریبا غیرقابل‌نفوذ دور این شهر کشید. طی جنگ تروآ یونانی‌ها به مدت ۱۰ سال تروآ را محاصره کرده بودند و نتوانسته بودند آن را فتح کنند. در آخر به بهانه صلح و اتمام محاصره یک اسب چوبی به عنوان هدیه برای مردم تروآ ارسال کردند. همان‌طور که می‌دانید این اسب یک مجسمه چوبی ساده نبود و سربازها داخل آن پنهان شده بودند تا در موقعیت مناسب دروازه‌های شهر را بر روی دیگر سربازها باز کنند و شهر را فتح کنند. مردم تروآ این اسب را قبول کرده و در شب سربازهای یونانی دروازه‌ها را باز کرده و شهر فتح می‌شود.

قبل از شروع و تحلیل سناریو باید گفته شود که موارد زیر اهداف اصلی حمله تروجان هستند:

- از کار انداختن دستگاه
- تماشای صفحه نمایش کاربر و فعال‌سازی وب‌کم و میکروفون
- کنترل سیستم کامپیوتری از راه دور
- دزدی بانکی
- استفاده بیش از حد از CPU و GPU
- استفاده از کامپیوتر آلوده به عنوان پروکسی برای کارهای غیرمجاز

در بسیاری از نام‌گذاری‌ها، فقط شباهت مراحل در نظر گرفته می‌شود اما در این مورد مراحل نفوذ دقیقا به همین صورت انجام می‌شوند. برای درک بهتر شباهت‌های بین داستان و نفوذ واقعی، یک سناریو تعریف می‌کنیم و نقش‌ها مشخص می‌شوند.

از آن‌جایی که حمله تروجان زیرمجموعه مهندسی اجتماعی است، بنابراین می‌توان گفت همه چیز از پشت میز صورت نمی‌گیرد و تا حدودی باید از هدف اطلاعاتی داشت تا حمله بهتری صورت بگیرد. برای تعریف سناریو، یک شخص فرضی به نام آقای ایکس در نظر می‌گیریم؛ آقای ایکس کارمند شرکتی در اصفهان است که خدمات پس از فروش محصولی را ارائه می‌دهند. اینجا دو حالت داریم، یا اینکه هکرها از قبل آقای ایکس را می‌شناسند و می‌دانند که این شخص علاقه بسیاری به خرید موبایل‌های جدید دارد؛ برای همین برای او یک لینک آلوده به یک بدافزار را ایمیل یا اس‌ام‌اس می‌کنند که نوشته است: با نصب اپلیکیشن تخفیف موبایل از آخرین تخفیفات موبایل فروشی‌های اصفهان مطلع شوید. به احتمال زیاد آقای ایکس به علت طمع و ذوق زیاد اپ را نصب کرده و بدافزار نصب می‌شود. از اینجا به بعد بستگی به هدف هکر دارد که چه کند. اگر هدف اطلاعات شرکت باشد، با کمی تلاش دیگر از طریق کامپیوتر یا موبایل آقای ایکس به آن‌ها دسترسی پیدا می‌کند. اگر هدف خوده آقای ایکس باشد توسط همان اپ نصبی اطلاعات مورد نیاز از او گرفته می‌شود.

حالا اگر فرض کنیم قرار باشد همه چیز از پشت میز انجام شود، اینجا دیگر آقای ایکس مهم نیست که چه شخصی است یا چه سمتی در شرکت دارد. فقط از این نام به عنوان کسی استفاده می‌شود که در شرکت مورد نظر یک کامپیوتر دارد. هکر یک ایمیل برای یکی از کارمندها یا کامپیوترش می‌فرستد که بر فرض ما کامپیوتر آقای ایکس است. این ایمیل ممکن است هر محتوایی داشته باشد که باعث واکنش سریع از طرف آقای ایکس شود. بر فرض مثال در ایمیل نوشته شده:

من از خدمات شرکت شما ناراضی هستم و دیگر از خدمات شما استفاده نخواهم کرد.

آقای ایکس واکنش نشان می‌دهد و علت را جویا می‌شود تا شاید بتواند هکر را راضی کند.

سپس از طرف هکر ایمیل دیگری دریافت می‌کند که: در لینک زیر وارد شوید و خدمات شرکت همکار رو ببینید و باعث تاسف است که شما این خدمات را ندارید. این‌جاست که آقای ایکس با تمام تلاش به دنبال علت‌ها می‌رود و برای این کار باید روی لینک کلیک کند و مانند سناریوی قبل، بقیه مسائل به خواسته هکر ربط دارند.

برویم به سراغ مقایسه؛ در سناریوها آقای ایکس هدف است؛ بنابراین می‌توان آقای ایکس را مردم یا شهر تروآ در نظر گرفت. هکر هم همان‌طور که مشخص است مهاجم می‌باشد، یعنی یونانی‌ها. هکر از چیزی استفاده می‌کند که هدف را مجبور به واکنش می‌کند همان‌طوری که یونانی‌ها اسب چوبی را فرستادند.

حصارها همان فایروال‌ها هستند که تا حدودی می‌توانند از ما محافظت کنند مگر این‌که خودمان باعث بشویم هکر آن‌ها را دور بزند.

در نتیجه همیشه باید به یاد داشت در هیچ صورتی نباید به پیامک‌ها یا ایمیل‌هایی که حاوی پیشنهادهای عالی هستند یا اینکه تهدید آمیز هستند واکنش سریع و بدون فکر داد زیرا به احتمال زیاد با یکی از روش‌های مهندسی اجتماعی قصد هک را دارند. بنابراین باید کمی فکر کرد و سپس در صورت لزوم به پلیس فتا اطلاع داد.

منبع:
- Antivirus, chipic.co

خبرهای مهم

گزیده اخبار فروردین‌ماه

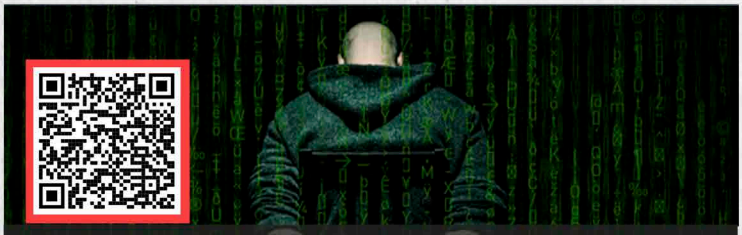
گردآورنده: سروش ذوالفقاری
zolfaghari.soroush@gmail.com

خرده‌فروشی بریتانیا به دنبال یک حمله سایبری مخرب تا حدی تعطیل شد.

فروشگاه زنجیره‌ای خرده‌فروشی کتاب، لوازم هنری و لوازم‌التحریر بریتانیا به نام The Works، در پی حمله سایبری به سیستم‌های کامپیوتری خود، مجبور شد چندین فروشگاه خود را ببندد و تحویل سهام جدید را متوقف کند. The Works که دارای ۵۲۶ فروشگاه در سراسر بریتانیا است، از یک حمله باج‌افزاری رنج می‌برد، اما به نظر می‌رسد که هکرها هنوز هیچ پاداش مالی برای داده‌های مورد دسترسی درخواست نکرده‌اند. در پی کشف این حادثه در هفته گذشته، پنج فروشگاه از صدها فروشگاه مجبور به تعطیلی شدند.

سوابق دادگاه بدون مهر و موم نشان می‌دهد که وزارت دادگستری ایالات متحده (DoJ) سه دامنه را که میزبان وب‌سایت RaidForums بودند، در اختیار گرفت. مقامات ایالات متحده مشارکت خود را در بستن RaidForums، بازار محبوب خرید و فروش داده‌های هک شده، تایید کردند.

RaidForums یک فروم محبوب مخصوص هکرها در دارک‌وب است که در آن تا اکنون صدها پایگاه داده سرقت شده به فروش رفته است.



ایالات متحده تصرف وب‌سایت RaidForums را تأیید می‌کند، مالک آن دستگیر شده است.

ایالات متحده بات‌نت اداره شده توسط سازمان اطلاعات روسیه را مختل می‌کند.

وزارت دادگستری ایالات متحده یک بات‌نت جهانی موجود در هزاران دستگاه سخت‌افزاری شبکه آلوده را که توسط بازیگر بدنام Sandworm کنترل می‌شد، مختل کرد. Sandworm به اداره اطلاعات اصلی ستاد کل نیروهای مسلح فدراسیون روسیه (GRU) نسبت داده می‌شود.

هکرهای جدی یا فقط یک دسته بچه اسکیریپتی

$Lapsus نام یک گروه هکری است که در سال جاری جزء فعال‌ترین گروه‌های سایبری بوده است و حملات بسیاری به شرکت‌های معروف و نام‌آور داشته‌اند.
بر اساس داده‌های جدیدی که امروز توسط تحلیل‌گر امنیت سایبری Digital Shadows منتشر شد، $Lapsus وضعیت خود را به عنوان یک گروه باج‌افزار جعل کرد و در مقیاس حملات خود به شدت اغراق کرد.
گزارشی که در ادامه به تحقیقات مایکروسافت استناد می‌کند نشان می‌دهد که در عوض بر تکنیک‌های مهندسی اجتماعی و جمع‌آوری اعتبار برای استخراج داده‌ها متکی است.
در این گزارش آمده: "در حالی که $Lapsus ادعا می‌کرد در حملات اولیه خود از باج‌افزار استفاده کرده است، هیچ مدرکی مبنی‌بر استفاده این گروه از بدافزار رمزگذاری وجود ندارد."

Nord Security برای اولین بار سرمایه خارجی خود را برای ساخت "اینترنت کاملاً بهتر" افزایش می‌دهد.

شرکت امنیت و حریم خصوصی اینترنت Nord Security گفته است که به دنبال یک رویکرد جامع‌تر به امنیت آنلاین است. Nord Security ۱۰۰ میلیون دلار جمع‌آوری کرده است و این تامین مالی توسط Nova-tor Ventures با مشارکت Burda Principal Investments و General Catalyst هدایت می‌شود. Nord Security از این بودجه برای گسترش مجموعه محصولات و ردپای سازمانی خود و تسریع رشد شرکت امنیت سایبری مصرف‌کننده Surfshark استفاده خواهد کرد.

Hydra بزرگ‌ترین بازار Dark Web جهان تعطیل و تصرف شد.

Hydra یکی از معروف‌ترین بازارهای سیاه اینترنتی منتسب به روسیه بود. حال مقامات آلمانی از توقیف زیرساخت سرور هایدرا خبر دادند و این بازار را تعطیل کردند. علاوه بر این، مقامات بیش از ۲۳ میلیون دلار بیت‌کوین منتسب به بازار را تصاحب کردند. این عملیات با هماهنگی سازمان‌های مجری قانون آمریکا و اروپا انجام شد. مقامات ادعا می‌کنند که این توقیف پیام را به مجرمان سایبری ارسال می‌کند که هیچ پناهگاه امنی برای پنهان شدن وجود ندارد.

مقایسه لینوکس و ویندوز در سرورها

اسب تروجان

امنیت سایبری در نیروگاه‌ها

Cyber news

روز صفرم ترجمه ی عبارت Zero Day می‌باشد که در تعبیر لغوی یعنی روزی که هنوز به آن نرسیده‌ایم و از وجود چنین چیزی هم خبر نداریم، وقتی صحبت از حمله Zero Day می‌شود یعنی در خصوص حمله ای صحبت می کنیم که هیچکس تا کنون آن را شناسایی نکرده است و هیچ دانشی هم در خصوص آن وجود ندارد که چگونه آن را تشخیص و بعضا از بروز آن جلوگیری کنیم.
در این نشریه سعی بر آن است تا زوایای پنهان و ناشناخته در دنیای امنیت اطلاعات مورد بررسی قرار گرفته و به جدیدترین اخبار و تکنولوژی‌های این حوزه پرداخته شود. مخاطبین این نشریه تمامی دانشجویان و افرادی خواهند بود که به حوزه امنیت اطلاعات علاقمند هستند.

برای ارسال مقالات جهت چاپ در نشریه به @elahe_rahbaran در تلگرام پیام دهید.