



**Namatek**  
True Education

# Check the security of the Linux

[www.namatek.com](http://www.namatek.com)

بررسی امنیت سیستم  
عامل لینوکس

## فهرست مطالب

1. میزان اهمیت سیستم عامل در امنیت
2. دلایل موثر در امنیت لینوکس

امنیت لینوکس در کنار منبع باز بودن آن دلیل استقبال از این سیستم عامل قوی است چرا که امنیت در دنیای امروز یک اصل مهم است. شاید شما هم شنیده باشید که یک جمله در دنیای امنیت وجود دارد که می گوید تنها سیستم کامپیوتر ایمن، سیستمی است که از هر شبکه ای جدا باشد، همچنین خاموش شده و شش فوت زیر زمین دفن شود.

در حال حاضر تعداد بیشتری از سیستم های رایانه ای به طور مستقیم یا از طریق شبکه های محلی به اینترنت متصل هستند که بیش از هر زمان دیگری در تاریخ فناوری در حال رشد است. در این بین طی یک ماه ممکن است چندین خبر در مورد به خطر افتادن شبکه داخلی یک شرکت بزرگ توسط متجاوزین منتشر شود. واقعیت ساده این است که تا زمانی که اتصال به یک شبکه وجود داشته باشد چیزی به نام یک سیستم واقعا امن وجود ندارد اما خوشبختانه همه چیز از بین نرفته است و ما مجبور نیستیم کابل های شبکه را از پشت سیستم های رایانه ای خود بیرون بیاوریم. با برنامه ریزی دقیق و پیکربندی سیستم، یک محیط امن که باعث می شود هکر به سمت هدف بعدی و آسانتر حرکت کند، وجود دارد.



## #1 میزان اهمیت سیستم عامل در امنیت

سیستم عاملی که برای خود نصب می کنید تفاوتی در موضع امنیتی شما ایجاد می کند اما یک محافظ مطمئن نیست. استقرار یک سیستم عامل امن یک نقطه شروع مهم است اما بدون آموزش کاربر، حتی با داشتن فایروال های قوی نیز مورد تهدید قرار می گیرد. در میان سیستم عامل ها امنیت لینوکس می تواند بخشی از امنیت شبکه ها، سرورها و سیستم ها را فراهم کند.



اما در این بین تخصص و اطلاع کاربر در حفظ این امنیت نقش مهمی دارد. به عنوان مثال در زمان بروزرسانی نرم افزار، نصب برنامه های افزودنی، برنامه های کمکی، افزونه ها و سایر نرم افزارهای بارگیری شده احتمال دسترسی غیر مجاز وجود دارد و سبب فعال سازی بدافزار در سیستم می شوند. همچنین دسترسی کاربر `root` در لینوکس و Administrator در ویندوز سیستم عامل شما را آسیب پذیرتر می کند. در ابتدای شروع به کار با سیستم عامل، بیاموزید که چگونه گذرواژه های امن انتخاب کنید و با ابزارهای مختلف مدیریت آشنا شوید که داشتن گذرواژه های مختلف در هر حساب و وب سایت برای شما راحت تر باشد.

## #2 دلایل موثر در امنیت لینوکس

کاربران لینوکس از لحاظ امنیتی دارای برخی مزایای ذاتی نسبت به سایر کاربران سیستم عامل ها مانند کاربران ویندوز هستند. هکرها به طور مداوم در تلاش برای یافتن سیستم های رایانه ای آسیب پذیر برای نفوذ هستند و از قوانین شانس و میانگین استفاده می کنند.



آن ها معمولا سیستم هایی را که بیشترین آسیب پذیری امنیتی را دارند را هدف قرار می دهند.

هکرها همچنین بیشترین توجه را به مناطقی متمرکز می کنند که بیشترین امکان برای وجود سیستم های محافظت نشده وجود دارد.

در این موارد سیستم عامل ویندوز آسیب پذیرتر بوده و سیستم عامل لینوکس از امنیت بیشتری برخوردار است.

در ادامه برخی از دلایل موثر در امنیت لینوکس را مورد بررسی قرار خواهیم داد.

## #2-1 عدم استقبال کاربران دسکتاپ با وجود امنیت

### لینوکس

احتمالا شنیده باشید که متخصصان اتفاق نظر دارند که لینوکس امن ترین سیستم عامل است اما با این حال که این سیستم عامل به دلیل امنیت بالا مورد نظر برای سرورها است، شرکت هایی که آن را روی دسک تاپ نصب می کنند بسیار کم هستند.

بیشترین دلیل ایمنی لینوکس به تعداد کم استفاده از آن مربوط می شود. در مقایسه با ویندوز که با بیش از ۸۰ درصد از کل دستگاه ها کار می کند، لینوکس کمتر از سه درصد بازار را دارد. بنابراین برای کسانی که نرم افزارهای مخرب ایجاد می کنند، هدف قرار دادن ویندوز منطقی تر است زیرا این قطعه کد مخرب به بزرگترین قشر جامعه (یعنی ۸۰ درصد از کاربران) آسیب می زند. همین امر باعث می شود کاربران لینوکس ایمن تر باشند.



## #2-2 توزیع های مختلف لینوکس

توزیع های لینوکس که امنیت را به عنوان یک ویژگی اصلی هدف قرار می دهند شامل Parrot Linux هستند.

یک توزیع کننده مبتنی بر دبیان می گوید بسیاری از ابزارهای مربوط به امنیت را فراهم می کند. به عقیده کترین نویز (Katherine Noyes) پژوهشگر امنیتی، وجود توزیع های مختلف نشانه بستر مناسب در ایجاد امنیت لینوکس است چرا که بعضی از آن ها به طرق مختلف موارد امنیتی را برقرار می کنند و با یکدیگر متفاوت هستند.

وجود این توزیع ها و روش های امنیتی مختلف در آن ها کار هکر ها را سخت تر کرده و امنیت بیشتری به این سیستم عامل می بخشد.

## #2-3 منبع باز و رایگان بودن لینوکس

لینوکس امن ترین سیستم عامل است، زیرا منبع آن باز است.

هر کسی می تواند آن را بررسی کند و اطمینان حاصل کند که هیچ اشکالی در پشت صحنه عملکرد آن وجود ندارد.

ویلیکینسون توضیح می دهد که "کد لینوکس توسط جامعه فناوری بررسی می شود و همین نظارت ها، آسیب پذیری ها، اشکالات و تهدیدهای کمتری را به وجود می آورد".



## #2-4 محدودیت دسترسی ها در لینوکس



یکی از عوامل ذکر شده توسط PC World ، مدل امتیازات بهتر کاربر Linux است:

طبق مقاله خانم نويز، دسترسی کاربران ویندوز به طور پیش فرض سطح دسترسی مدیر است. به این معنی که کاربران سیستم عامل ویندوز تقریباً به همه چیزهای سیستم دسترسی دارند. این موضوع امنیت وینوز را تا حد زیادی پایین می آورد اما در مقابل لینوکس دسترسی را بسیار محدودتر می کند.

## #2-5 دشوارتر بودن اجرای پیوست خطرناک در

### لینوکس

اگر با لینوکس کار نکرده باشید، ممکن است متوجه نشوید که عملکرد آن مشابه Windows یا Mac نیست. در این سیستم عامل ها باز کردن یک پیوست خطرناک صرفا با دوبار کلیک انجام می شود اما در لینوکس قبل از اجرای یک نرم افزار مخرب مراحل دیگری نیز باید طی شود.

کاربران لینوکس باید پیوست را قبل از اجرای پیوست آن ذخیره کنند و در صورت تنظیم صحیح امکان اجرا وجود خواهد داشت. این مراحل اضافی می تواند به محافظت از مشاغل در مقابل کاربر داخلی Kill که اغلب دلیل نقض امنیت است، کمک کند.

## #2-6 توسعه دهندگان جهانی امنیت لینوکس

اگرچه مایکروسافت دارای ارتشی از توسعه دهندگان است که روی این سیستم عامل کار می کنند اما تعداد توسعه دهندگانی که روی لینوکس کار می کنند بیشتر است. این یکی از بزرگترین دلایل امنیت لینوکس است.



کاترین نویز در این زمینه توضیح می دهد که "مایکروسافت ممکن است تیم بزرگی از توسعه دهندگان پولی خود را تبلیغ کند اما بعید است که این تیم بتواند خود را با پایگاه جهانی توسعه دهندگان کاربران لینوکس در سراسر جهان مقایسه کند. بخش بزرگی از امنیت لینوکس از این طریق حاصل می شود".

با توجه به اینکه افراد زیادی مشکلات را در امنیت لینوکس رصد می کنند، در بیشتر اوقات مدت ها قبل از اینکه هکرها بتوانند آن را هدف قرار دهند آسیب پذیری پیدا شده و رفع می شود. همچنین پس از مشاهده مشکل، کاربران لینوکس مجبور نیستند ماه ها منتظر بمانند تا مایکروسافت سرانجام مسئله را بررسی کند و آن را برطرف کند. آن ها خودشان می توانند از هرجایی که هستند آن را تعمیر کنند. این نه تنها امنیت لینوکس را بهبود می بخشد، بلکه هر مشکل و خرابی را رفع کرده و وضعیت کارها را ثابت نگه می دارد.