# امن‌سازی سیستم‌عامل‌های مایکروسافت ویندوز ۷ و اندروید



مؤلفین:
دکتر بابک صادقیان
گوهر شکوری گرکانی

سرشناسه : صادقیان، بابک، ۱۳۴۰-
عنوان و نام پدیدآور : امن‌سازی سیستم‌عامل‌های مایکروسافت ویندوز ۷ و اندروید
مولفین بابک صادقیان، گوهر شکوری گرکانی
مشخصات نشر : تهران: انتشارات ناقوس، ۱۳۹۴.
مشخصات ظاهری : ۱۷۸ ص.: مصور، جدول.
شابک : ۰-۷۹۲-۳۷۷-۹۶۴- ۹۷۸ بها : ۱۵۰،۰۰۰ریال به همراه DVD
وضعیت فهرست‌نویسی : فیپای
یادداشت : کتابنامه: ص ۱۶۷-۱۷۰.
موضوع : ویندوز مایکروسافت—اقدامات تامینی
موضوع : اندروید (منبع الکترونیکی)— تدابیر ایمنی
موضوع : سیستم‌های عامل(کامپیوتر)—تدابیر ایمنی
شناسه افزوده : شکوری گرکانی، گوهر، ۱۳۶۵-
رده‌بندی کنگره : ۱۳۹۴ ۲۲ص۹۴س/QA۷۶/۷۶
رده‌بندی دیویی : ۰۰۵/۸
شمارهٔ کتابشناسی ملی : ۳۹۲۶۳۶۰



چاپ اول

| | |
|---|---|
| نام کتاب | : امن‌سازی سیستم‌عامل‌های مایکروسافت ویندوز ۷و اندروید |
| ناشر | : انتشارات ناقوس |
| تالیف | : بابک صادقیان، گوهر شکوری گرکانی |
| چاپ اول | : ۱۳۹۴ |
| تیراژ | : ۲۰۰ جلد |
| چاپ و صحافی | : نارنجستان |
| سرپرست صفحه‌آرا | : صدف پورعبدی |
| قیمت با DVD همراه | : ۱۵۰،۰۰۰ریال |
| شابک | : ۰-۷۹۲-۳۷۷-۹۶۴- ۹۷۸ |
| ISBN | : 978-964-377-792-0 |

S.M.S : ۳۰۰۰۴۵۲۳۲۳



مرکز پخش: انتشارات ناقوس
۱-میدان انقلاب، خیابان کارگرجنوبی، خیابان ۱۲ فروردین- بین وحیدنظری و روانمهر- بن‌بست حقیقت- پلاک ۴
تلفن و فاکس : ۶۳۴۲۵ (۲۰خط)
۲- کتابفروشی الیاس: خیابان انقلاب، نبش ۱۲ فروردین تلفن: ۶۶۴۰۵۰۸۴
۳- کتابفروشی گلریزان: ضلع جنوب‌شرقی میدان انقلاب، پلاک ۱۱ تلفن: ۶۶۹۷۶۲۳۰

# فهرست مطالب

# پیشگفتار

در مباحث مربوط به مهندسی کامپیوتر اصطلاح Hardening برای فرآیند مستحکم کردن یک سیستم با کاهش سطح آسیب‌پذیری آن به‌کار می‌رود. اگر ترجمه لغوی این اصطلاح را در نظر بگیریم بایستی آنرا به سخت‌سازی یا مُستحکم‌سازی ترجمه کرد، ولی در میان افراد فنی کامپیوتری در ایران این اصطلاح معمولاً با عبارت «امن سازی» معادل‌سازی می‌گردد. از آنجاکه این کتاب برای افراد فنی نوشته می‌شود، ما نیز در این کتاب از اصطلاح امن‌سازی استفاده می‌کنیم. امّا سطح آسیب‌پذیری یک محیط نرم‌افزاری یا Surface of Vulnerability یا سطح آسیب‌پذیری به مجموع نقاط مختلفی که یک کاربر غیرمجاز می‌تواند سعی در ورود داده و/ یا استخراج داده از آن محیط مورد نظر کند، گفته می‌شود.

نمونه‌هایی از چنین نقاطی: فیلدها، واسط‌ها، پروتکل‌ها و سرویس‌های ورود کاربر است. مسلماً هر چه‌قدر یک سیستم کارهای بیشتری انجام دهد سطح آسیب‌پذیری بزرگتری دارد؛ از طرفی یک سیستم تک‌عملکردی محکمتر از یک سیستم چندعملکردی است. از این‌رو، یک رویکرد برای بهبود امنیت اطلاعات، کاستن سطح آسیب‌پذیری یک سیستم یا نرم‌افزاراست. استراتژی‌های اصلی برای کاهش سطح آسیب‌پذیری عبارتند از: کاستن از مقدار کد در حال اجرا و حذف نرم‌افزارهای غیر ضروری، کاستن از نقاط ورود در دسترس کاربرانی که اعتمادی به آنها نیست و نام‌های کاربری غیرضروری، و حذف سرویس‌هایی که نسبتاً متقاضی ندارند.

شیوه‌های مختلفی برای مستحکم‌سازی سیستم وجود دارد. این اقدامات ممکن است شامل به‌کارگیری وصله‌های نرم‌افزاری (یا patch)، بستن پورت‌های شبکه‌ای باز، و راه‌اندازی سیستم‌های تشخیص نفوذ، فایروال، و سیستم‌های جلوگیری از نفوذ باشد. همچنین، ابزارها و برنامه‌های نوشته‌شده‌ای وجود دارند که خصوصیات غیرلازم را در فایل پیکربندی غیرفعال کرده یا اقدامات پیشگیرانه مختلف دیگری را انجام می‌دهند. به هر حال توجه به این نکته ضروری است که اگرچه کاستن سطح آسیب‌پذیری به جلوگیری از شکست امنیتی کمک می‌کند، ولی میزان صدمه و خسارتی را که یک مهاجم -که آسیب پذیری را پیدا کرده است- وارد می‌کند کاهش نمی‌دهد.

فرآیند Hardening بخشی از مدیریت حوادث امنیتی کامپیوتر ( Computer Security Incident Management) است، که تیم‌های پاسخ به حوادث امنیتی کامپیوتر یا CSIRT ( Computer Security Incident Response Team) ها به آن می‌پردازند.

کتاب حاصل نتیجه بخشی از مطالعاتی است که در مرکز پژوهشی آپای دانشگاه صنعتی امیرکبیر طی قراردادی که به منظور حمایت از مطالعات این حوزه توسط ستاد ICT معاونت علمی و فناوری ریاست جمهوری در سال ۱۳۹۱ منعقد گردید صورت گرفته است. در بخشی از این مطالعات قرار بود که بسته آموزشی برای امن‌سازی دو سیستم عامل تهیه گردد. فرصت پیش آمده بهانه‌ای شد تا امن‌سازی چهار سیستم عامل متداول Windows Server 2008، Windows 7، Ubuntu Server و Android مورد مطالعه قرار گیرد و بسته آموزشی برای امن‌سازی آنها تهیه گردد. بدین منظور، ابتدا اطلاعات

لازم با استفاده از منابع در دسترس اینترنتی مطابق سرفصل تهیه شده جمع‌آوری گردید و سپس اطلاعات جمع‌آوری‌شده روی سیستم‌های واقعی امتحان شد. پس از آن، مطالب نوشته‌شده تکمیل و مورد بازبینی قرار گرفتند. تهیه اسلاید، تهیه تصاویر آموزشی، تنظیم مطالب برای قرائت، صدابرداری، صداگذاری روی اسلایدها و تهیه ویدئوی آموزشی مراحل مختلفی بودند که تیم مطالعاتی برای تهیه بسته آموزشی طی کرد. عزیزانی که در این فعالیت همکاری کردند شامل جناب دکتر رضا سپهی، خانم مهندس فرشته جعفری، خانم مهندس مهشید نوابی و خانم مهندس پروانه آقاجانی بودند که به‌صورت پاره‌وقت به بررسی‌های مربوطه و فعالیت‌های مربوط به تهیه بسته آموزشی پرداختند. اگر چه مناعت این عزیزان مانع از آن شد تا نام آنها بر روی جلد کتاب ظاهر گردد، در اینجا بر خود لازم می‌دانیم از تمامی این عزیزان که حداکثر تلاش خود را برای تهیه کاری ارزنده انجام دادند سپاسگزاری و قدردانی نماییم. همچنین، بر خود لازم می‌دانیم از جناب آقای دکتر محامدپور ریاست وقت ستاد ICT مذکور، جناب آقای مهندس جعفری و جناب آقای مهندس سجادی که قرارداد حمایتی با توجهات آنان به ثمر نشست تشکر و قدردانی نماییم.

# مقدمه مؤلف

امن‌سازی[1] سیستم‌های کامپیوتری به معنای کاهش آسیب‌پذیری‌های این سیستم‌ها با هدف به حداقل رساندن ریسک‌های امنیتی است. به‌صورت کلی، امن‌سازی سیستم‌های کامپیوتری در چهار سطح زیر انجام می‌پذیرد:

- امن‌سازی فیزیکی
- امن‌سازی سیستم‌عامل
- امن‌سازی شبکه
- امن‌سازی برنامه‌های کاربردی

موضوع اصلی این کتاب، امن‌سازی سیستم‌عامل است که می‌تواند شامل موارد مختلفی مانند تغییر تنظیمات پیش‌فرض سیستم‌عامل، حذف سرویس‌ها و نرم‌افزارهای غیرضروری، حذف حساب‌ها و گروه‌های کاربری غیرضروری، رمزگذاری داده‌ها، رویدادنگاری، انجام بازرسی، نصب آنتی‌ویروس، نصب و تنظیم فایروال، به‌روزرسانی سیستم‌عامل و برنامه‌های نصب‌شده بر روی آن، و مواردی از این قبیل باشد.

این کتاب شامل خط‌مشی‌ها، سناریوها و دستورالعمل‌هایی جهت ایجاد امن‌سازی مایکروسافت ویندوز ۷ و سیستم‌عامل اندروید است. توصیه‌ها و دستورالعمل‌های مطرح‌شده در این کتاب تا حدی اطمینان می‌دهد که کامپیوترهای استفاده‌کننده از این سیستم‌عامل در برابر تهدیدات رایج امنیتی ایمن هستند.

---

[1] Hardening