

آسیب‌پذیری‌های امنیتی

مهاجر تل‌ف‌ن خصوصی

مؤلف: یاسر ایزدی

www.ketab.ir

سرشناسه: ایزدی، یاسر، ۱۳۵۹

عنوان و نام پدیدآور: آسیب‌پذیری‌های امنیتی مراکز تلفن خصوصی / مولف: یاسر ایزدی
مشخصات نشر: تهران، انتشارات دیده‌بان، ۱۳۹۳
مشخصات ظاهری: ۸۲ صص، مصور، جدول، نمودار
وضعیت فهرست‌نویسی: فیا
یادداشت: -

موضوع: تلفن، سیستم‌ها، تدابیر امنیتی، انشعاب فرعی، تکنولوژی اطلاعات و ارتباطات، ایران
رده‌بندی کنگره: ۱۳۹۳ ۹۱۵/الف TK۶۴۰۱
رده‌بندی دیویی: ۶۵۱/۷۳ کتابشناسی ملی: ۳۶۰۹۹۷۰



انتشارات دیده‌بان

❖ عنوان کتاب: آسیب‌پذیری‌های امنیتی مراکز تلفن خصوصی

❖ مولف: یاسر ایزدی

❖ ناشر: انتشارات دیده‌بان

❖ ویراستار علمی: جواد بزرگی

❖ ویراستار ادبی: میترا مشهدی رجب

❖ ناظر علمی: امیر جعفرقلی

❖ طرح روی جلد: رضا حسنی

❖ لیتوگرافی، چاپ و صحافی: چاپ و نشر دانشگاه

❖ شمارگان: ۱۰۰۰ جلد

❖ نوبت چاپ: اول، پاییز ۹۳

❖ قیمت: ۸۰۰۰۰ ریال

ISBN: 978-600-93837-5-7

شابک: ۹۷۸-۶۰۰-۹۳۸۳۷-۵-۷

حق چاپ برای ناشر محفوظ است

آدرس: تهران، چهارراه پاسداران، انتشارات دیده‌بان، تلفن: ۲۳۱۱۲۲۳۱

فهرست مطالب

پیشگفتار.....	أ
یادداشت مولف.....	ج
فصل اول: ساختار و ویژگی‌های مراکز تلفن خصوصی.....	۱
ساختار و بلوک دیاگرام مراکز تلفن.....	۱
اصطلاحات و روش‌های خاص مراکز تلفن.....	۴
سخت‌افزار.....	۸
نرم‌افزار.....	۱۰
فصل دوم: انواع تهدیدات و آسیب‌پذیری‌های امنیتی در مراکز تلفن.....	۱۳
ارتباط امن و پایدار.....	۱۳
تهدیدات علیه ارکان امنیت اطلاعات.....	۱۴
فصل سوم: روش‌های نفوذ و اختلال در مراکز تلفن و راه مقابله.....	۱۹
روش‌های نفوذ و اختلال در مراکز تلفن.....	۲۴
ضعف‌های امنیتی مبتنی بر ساختار مراکز.....	۲۷
ضعف‌های امنیتی مبتنی بر سخت‌افزار.....	۳۰
ضعف‌های امنیتی مبتنی بر ترمینال‌های نگهداری و مدیریت.....	۳۵
ضعف‌های امنیتی مبتنی بر نرم‌افزار و قابلیت‌های مشترکین.....	۴۲
ضعف‌های امنیتی مبتنی بر مسیرهای صوت و سیگنالینگ.....	۶۸
منابع:.....	۷۹
ضمائم: چک لیست امنیتی مراکز تلفن.....	۸۰

پیشگفتار ناشر

طی سال‌های اخیر، توسعه شبکه‌های مخابراتی ثابت و سیار و ارائه سرویس‌های جانبی متعدد و جذاب، نیاز به راه‌های این شبکه‌ها، اگر چه موجب رضایت‌مندی بیشتر استفاده‌کنندگان شده است، اما من پیشرفت‌ها و خدمات می‌تواند موجب آسیب‌پذیری و بروز تهدیدات امنیتی برای استفاده‌کنندگان گردد. در همین رابطه هر روزه اخبار و اطلاعاتی از نفوذ افراد حاکم و هکرها به شبکه‌های اطلاعاتی و مخابراتی سازمان‌ها و ایجاد اختلال در عملکرد این شبکه‌ها مخابره می‌گردد. مراکز تلفن عمومی^۱ (PSTN) و خصوصی^۲ (PBX) به عنوان بخش عمده‌ای از زیر ساخت تبادل و انتقال اطلاعات و مکالمات تلفنی، همواره در معرض تهدیدات امنیتی و سوءاستفاده می‌باشند. یک PBX مرکز تلفنی است که جهت برقراری ارتباطات شرکت‌ها به صورت مستقل از شبکه مخابرات کشور مورد استفاده قرار می‌گیرد و با این طریق خطوط ترانک به شبکه مخابرات عمومی کشور متصل می‌شود. دلیل عمده انتقال از مراکز تلفن PBX کاهش هزینه‌های ارتباط تلفنی، حفظ امنیت اطلاعات و نیز ارائه سرویس‌ها و قابلیت‌های خاص (مانند انتقال مکالمه، برگشت مکالمه، کنفرانس و ...)

1- Public Switched Telephone Network

2- Private Branch Exchange

به استفاده‌کنندگان می‌باشد. با توجه به این‌که سازمان‌ها و شرکت‌های خصوصی اطلاعات مهم و کلیدی خود را از طریق این مراکز تبادل می‌کنند، هرگونه سرقت و یا شنود اطلاعات و یا اختلال در عملکرد این مراکز می‌تواند صدمات جبران‌ناپذیری به استفاده‌کنندگان وارد نماید.

استراق سمع و شنود مکالمات و نیز سوءاستفاده از خطوط تلفن PBX جهت برقراری تماس تلفنی به شکل قانونی و رایگان، از جمله حملات متداول به مراکز تلفن خصوصی می‌باشند. علاوه بر مکالمات صوتی، خطوط دورنگار و مودم و به دنبال آن دیسک‌های سازمان نیز قابل ذخیره‌سازی و شنود توسط نفوذکننده به مرکز تلفن می‌باشند. در دنیای امروز، اطلاعات، پایه و اساس رشد اقتصادی و رقابت در بازار برای شرکت‌ها و سازمان‌ها و پس از آن بعد کلان رشد و توسعه کشورها می‌باشد، مراقبت از اطلاعات مهم و کلیدی و نیز حفظ امنیت بسترهای ارتباطی حائز اهمیت دوچندان می‌باشد.

از آنجا که مراکز تلفن کم‌ظرفیت‌ترین مراکز در سازمان‌های دولتی و غیردولتی به وفور مورد استفاده قرار می‌گیرند و برخی مکان‌ها هستند که این مراکز استفاده می‌شوند از طبقه‌بندی اطلاعات بالایی برخوردارند، حفظ امنیت این مراکز و مکالمات تبادل‌شده در این بسترها ضروری می‌باشد.

در این کتاب به بررسی ضعف‌های امنیتی مراکز تلفن کم‌ظرفیت خصوصی پرداخته می‌شود و برخی راهکارهای مقابله به این ایرادات ارائه می‌شود. اما استخواندگان محترم با مطالعه مطالب ارائه‌شده نگاه جامع‌تری نسبت به ضعف‌های امنیتی مراکز تلفن PBX حاصل نموده و در جهت رفع ضعف‌های امنیتی مراکز تلفن مذکور تا حد امکان اقدام نمایند.