بسم الله الرحمن الرحیم

دانشگاه فردوسی مشهد
آزمایشگاه تخصصی آپا

وزارت ارتباطات و فناوری اطلاعات
سازمان فناوری اطلاعات ایران

مرکز ماهر
مرکز مدیریت امداد و هماهنگی عملیات رخدادهای رایانه‌ای

امنیت فناوری اطلاعات و ارتباطات؛
ضرورت‌ها و روندها

احسان طیرانی راد
مدیر آموزش و روابط‌عمومی آزمایشگاه تخصصی آپا
دانشگاه فردوسی مشهد

سمینار آموزشی مدیران و کارشناسان فناوری اطلاعات و ارتباطات استان آذربایجان غربی – ۲۶ مرداد ۱۳۹۵

امام صادق علیه‌السلام:

راز و اسرار تو به منزله‌ی خون توست، پس سعی کن که جز در شاهرگهایت به جریان نیفتند.

امنیت فناوری اطلاعات و ارتباطات

مفاهیم

عصر اطلاعات

- نقش فزاینده اطلاعات در جهان امروز
- پیشرفت سریع فناوری‌ها، رشد و توسعه علوم به‌واسطه دسترسی همگانی به اطلاعات
- فناوری اطلاعات به عنوان عامل تغییر
- حیاتی‌بودن تولید اطلاعات، دانش و علم و اهمیت حفظ و نگهداری از آن‌ها در عصر اطلاعات

اطلاعات و بهره‌گیری و تبدیل آن به دانش و خرد؛
عامل مزیت رقابتی برای اشخاص، سازمان‌ها و . . .

ویژگی‌های عصر اطلاعات

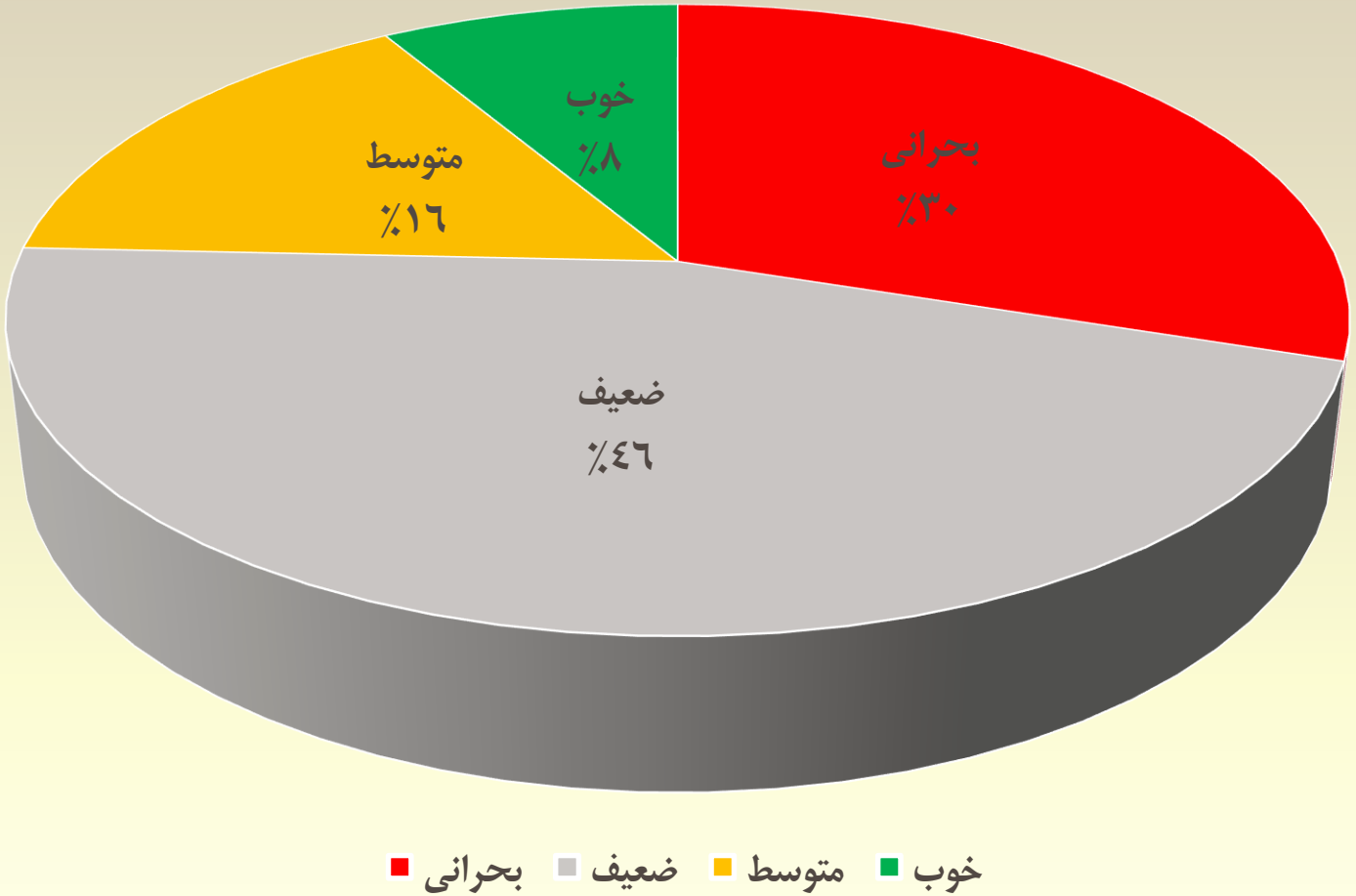
- اطلاعات، دارایی است
- سرمایه این عصر دارایی‌های نامشهود هستند (تحقیق و پژوهش، مهارت، دانش، فناوری و نوآوری)
- جامعه‌ای در این شرایط سرآمد است که بر اساس دانش و اطلاعات پایه‌ریزی شده باشد
- اکثر کسب‌وکارها بر اساس فناوری اطلاعات است و تاثیر بسیاری بر افزایش بهره‌وری فعالیت‌ها دارد

بنابراین امنیت اطلاعات موضوعی حیاتی برای همگان است

برخی گزارش‌ها و تحلیل‌های امنیتی در سال‌های ۲۰۱٤ و ۲۰۱۵

وضع موجود

نمونه گزارش آماری از وضعیت شبکه و زیرساخت در یک کره دیگر!!

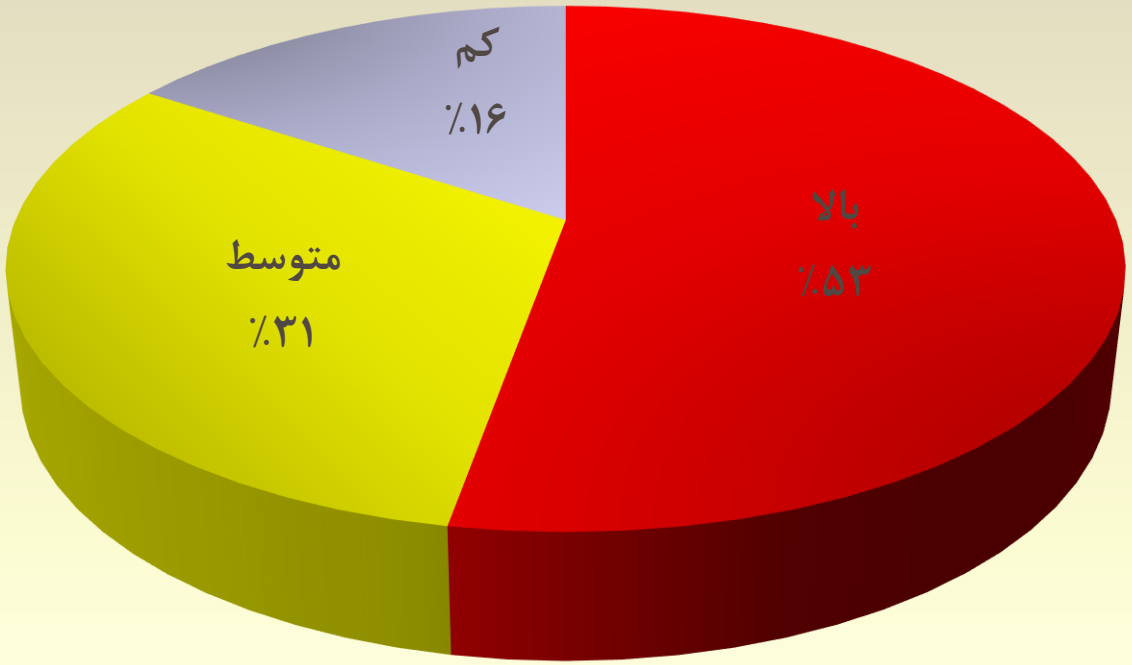


گزارش تحلیلی وضعیت همان شبکه همان کره دیگر!!

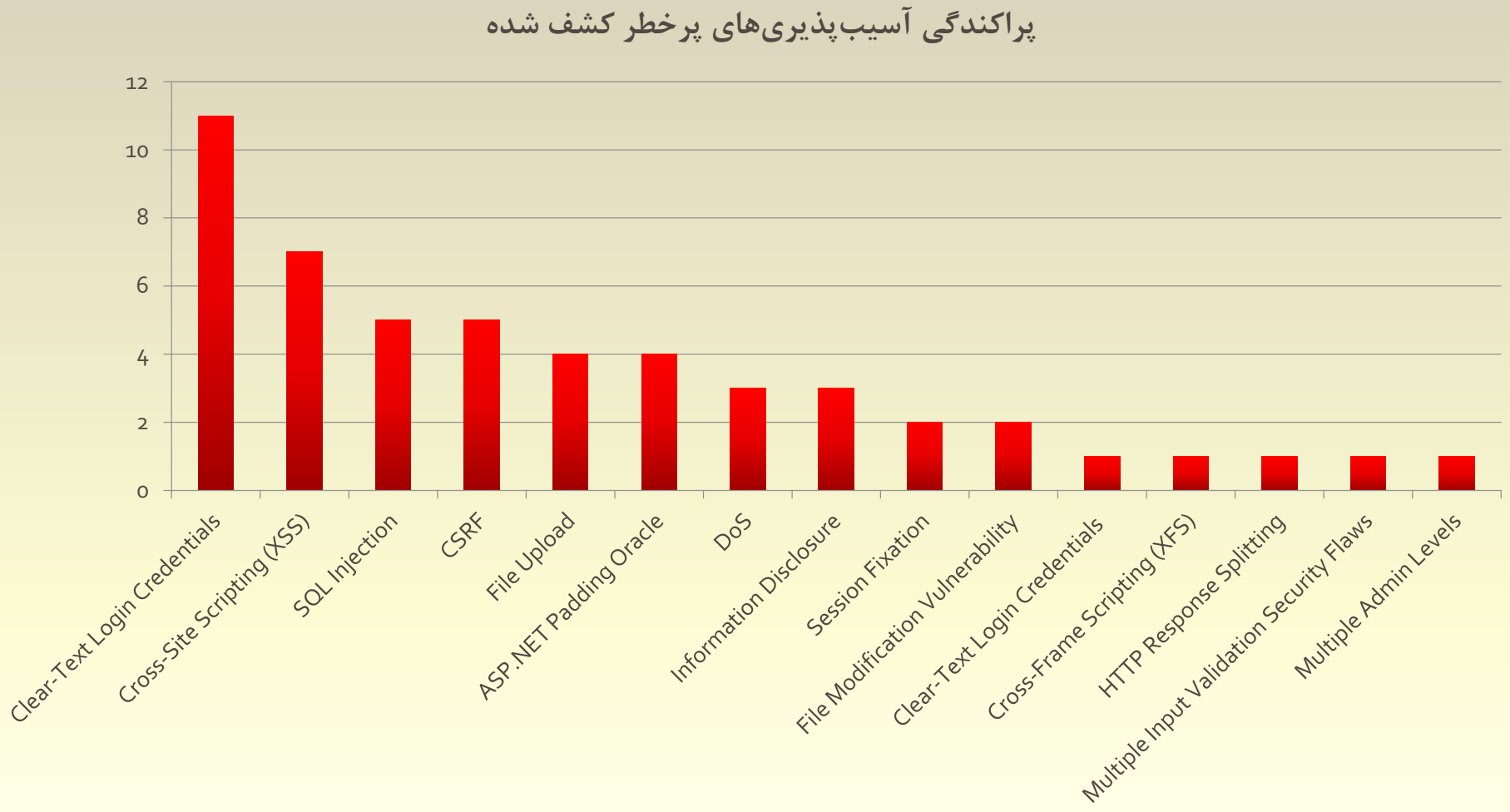
- نقص در طراحی و عدم دانش فنی مناسب در پیکربندی
- عدم استفاده بهینه از امکانات و تجهیزات
- نبود امکانات، تجهیزات و زیرساخت‌های مناسب
- عدم به کارگیری مشاوره‌ها و نظارت‌های فنی

نمونه گزارش وضعیت برنامه‌های کاربردی همان کره دیگر!!

سطح آسیب‌پذیری‌ها در پرتال‌ها و نرم‌افزارهای کاربردی



گزارش تحلیلی وضعیت همان برنامه‌های کاربردی همان کره دیگر!!



گزارش تحلیلی وضعیت همان برنامه‌های کاربردی همان کره دیگر!!

- عدم دانش امنیتی مناسب در تیم‌های برنامه‌نویسی

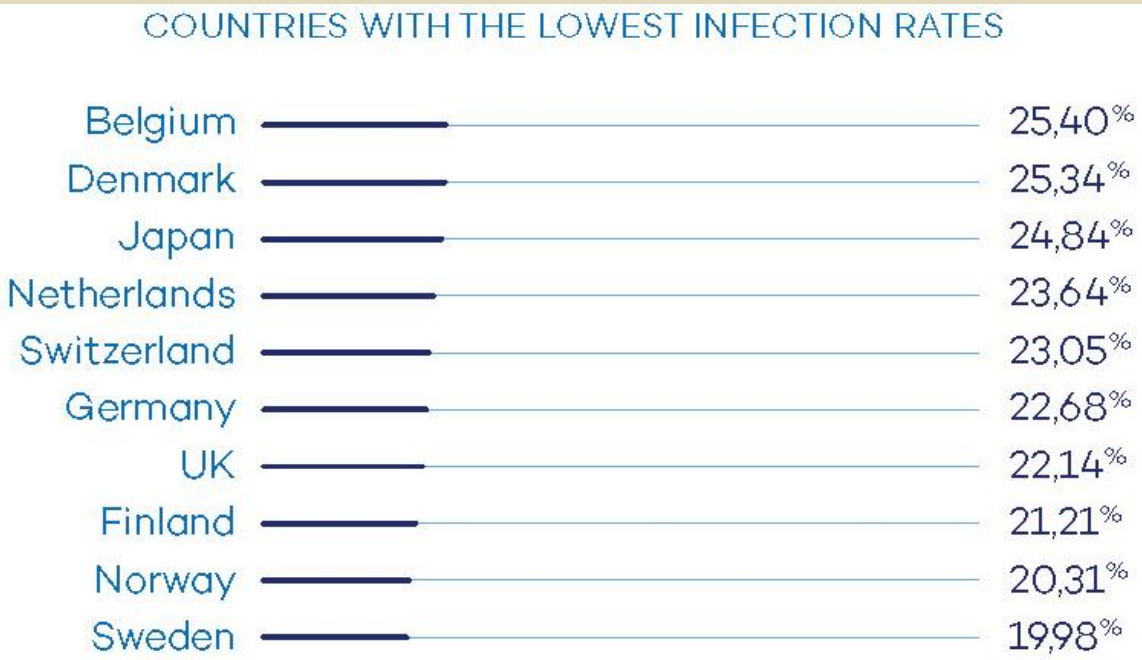
- صرف زمان طولانی در رفع مشکلات امنیتی از سوی شرکت‌ها

گزارش امنیتی شرکت پاندا در سال ۲۰۱۵

- **رشد چشمگیر بدافزارها**
- شناسایی روزانه ۲۳۰هزار بدافزار جدید
- از نظر این شرکت، سال ۲۰۱۴ یکی از بدترین سال‌ها در زمینه امنیت رایانه‌ای بود

گزارش امنیتی شرکت پاندا در سال ۲۰۱۵

- فهرست ۱۰ کشور با بیشترین نرخ آلودگی در سال ۲۰۱۴



- بالاترین موقعیت‌ها در این فهرست متعلق به کشورهای آسیایی و کشورهای آمریکای لاتین است. در مقابل، اروپا منطقه‌ای با پایین ترین نرخ آلودگی است.

گزارش امنیتی شرکت پاندا در سال ۲۰۱۵

- **یکی از مهمترین حمله‌های سایبری در سال ۲۰۱۵ مربوط به باج‌افزار و به‌طور خاص کریپتولاکر می‌شود.**

- این نوع حملات روی تمامی کاربران تاثیرگذار است، البته تاثیر آن روی شرکت‌هایی که اطلاعات با ارزشی نگهداری می‌کنند و حاضرند برای آن باج بدهند بیشتر است.

گزارش امنیتی شرکت پاندا در سال ۲۰۱۵

- در ماه فوریه شرکت آمریکایی Anthem اعلام کرد که قربانی حمله‌ای شده است که طی آن اطلاعات ۸۰ میلیون کاربر آن دزدیده شده است.

- حمله‌کنندگان با استفاده از یک نام و گذرواژه دزدی توانسته بودند به پایگاه داده شرکت دسترسی پیدا کنند و حدود ۱۰۰ میلیون دلار به این شرکت خسارت وارد کنند.

گزارش امنیتی شرکت پاندا در سال ۲۰۱۵

- هنگامی که ما در مورد حملات سایبری صبحت می‌کنیم، معمولاً به کامپیوترها، گوشی‌های هوشمند و تبلت‌ها فکر می‌کنیم. در حالی‌که سایر دستگاه‌های سخت‌افزاری نیز می‌توانند تحت تأثیر این حملات قرار گیرند.

- یک نقص امنیتی در روترهای Linksys به مهاجمین اجازه می داد که عملیاتی مانند تغییر تنظیمات DNS روتر را انجام دهند.

گزارش امنیتی شرکت پاندا در سال ۲۰۱٤

- مدت کوتاهی پس از انتشار خبر گم شدن هواپیمای مالزی، مجرمان سایبری شروع به انتشار لینکی روی فیس بوک کردند که ادعا می‌کردند ویدیویی از این هواپیما است. اما هنگامی که کاربر روی این لینک کلیک می کرد، کلمه عبور از وی درخواست می‌شد و به این ترتیب حساب وی مورد سرقت قرار می‌گرفت. اندکی بعد همین ترفند روی توییتر هم اجرا شد.

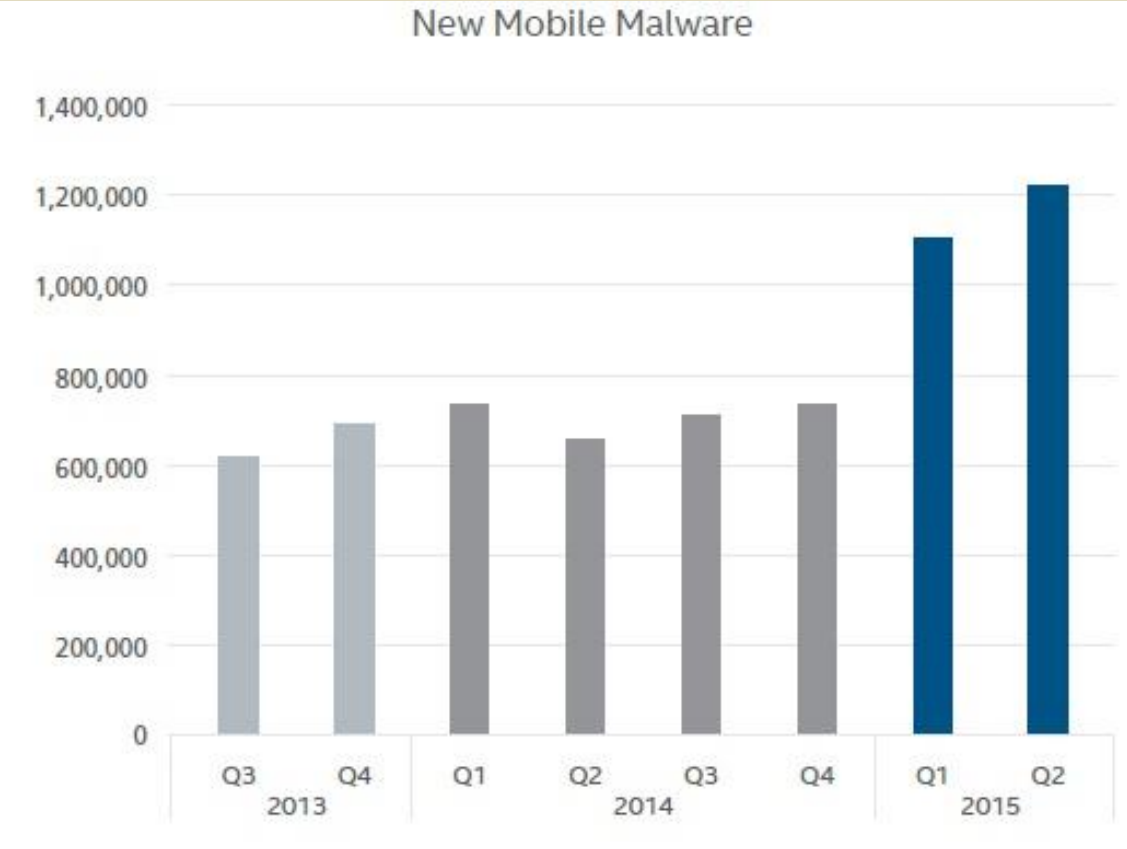
- همین حملات به صورت ایمیلی نیز تکرار شدند. این ایمیل ادعا می‌کرد که حاوی آخرین مکالمات خلبان با برج مراقبت دقایقی پیش از قطع ارتباط برج با هواپیما است.

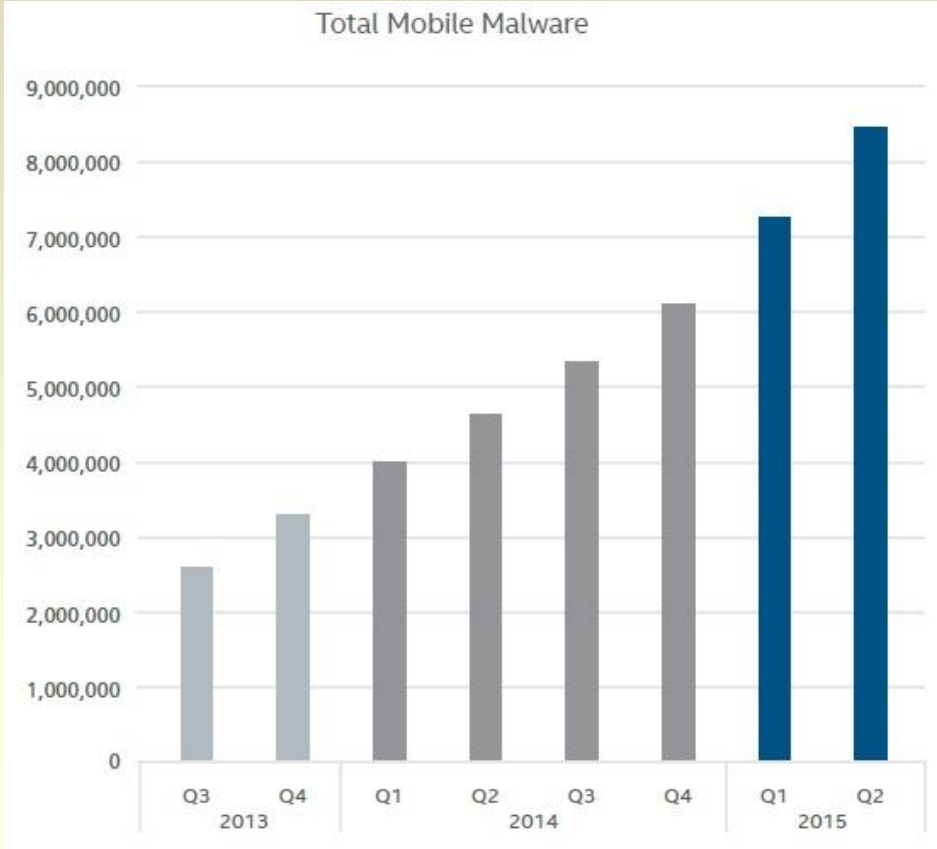
گزارش امنیتی شرکت پاندا در سال ۲۰۱٤

- در حوزه بدافزارهای موبایل در سال ۲۰۱۴ و در ماه فوریه پاندا چهار برنامه بدافزار در گوگل پلی کشف کرد. این برنامه‌ها که موضوعاتی مانند رژیم غذایی و مدل مو داشتند، کاربر را در سرویس‌های پولی ثبت‌نام می‌کردند و حتی اس ام اس های دریافتی از این سرویس‌ها را نیز پنهان می‌کردند تا کاربر تا زمان دریافت صورتحساب تلفن خود، متوجه موضوع نگردد. این برنامه ها در طول مدت یک ماه بین ۳۰۰ هزار تا ۱ میلیون و ۲۰۰ هزار مورد دانلود داشتند.
- در حمله مشابهی به جای گوگل پلی، مهاجمان صفحه‌ای مشابه آن طراحی کرده بودند و با تبلیغات در فیس بوک، کاربران را به آنجا می کشاندند.

گزارش امنیتی شرکت مک‌آفی در نیمه اول سال ۲۰۱۵

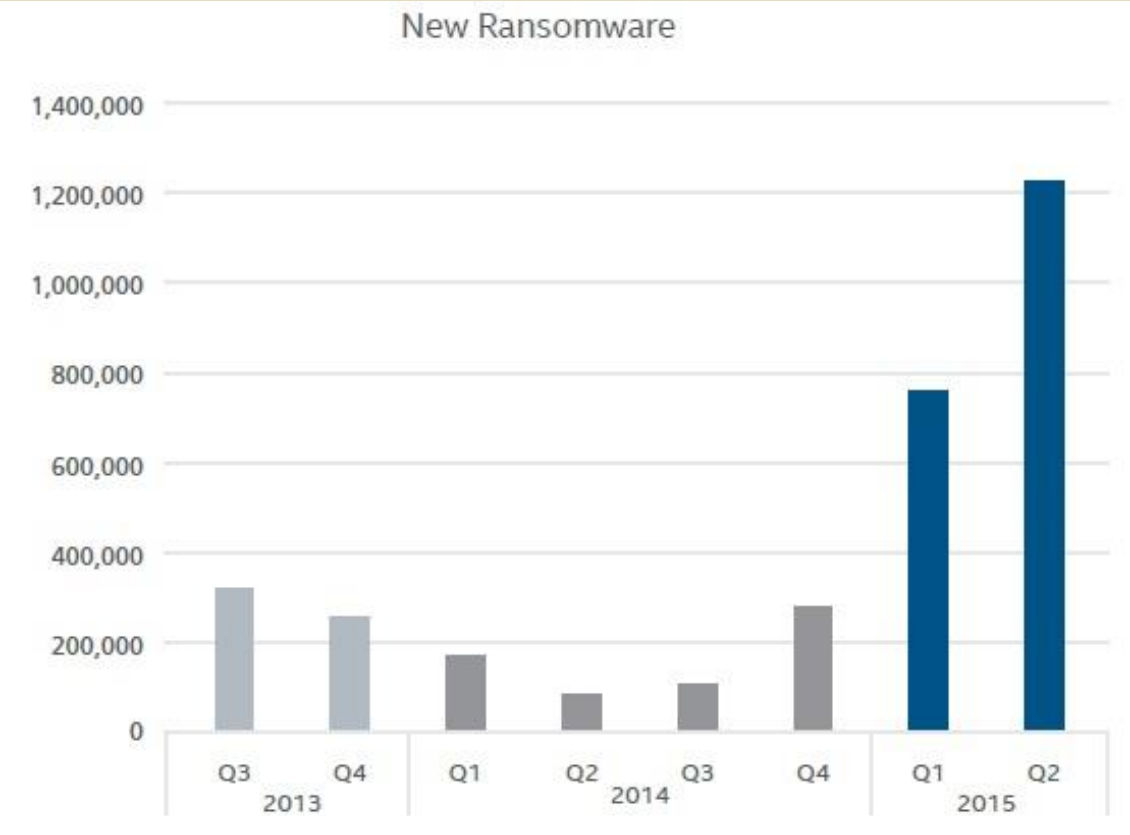
- تعداد کلی بدافزارهای تلفن همراه در سه ماهه دوم سال حدود ۱۷ درصد رشد داشته است.

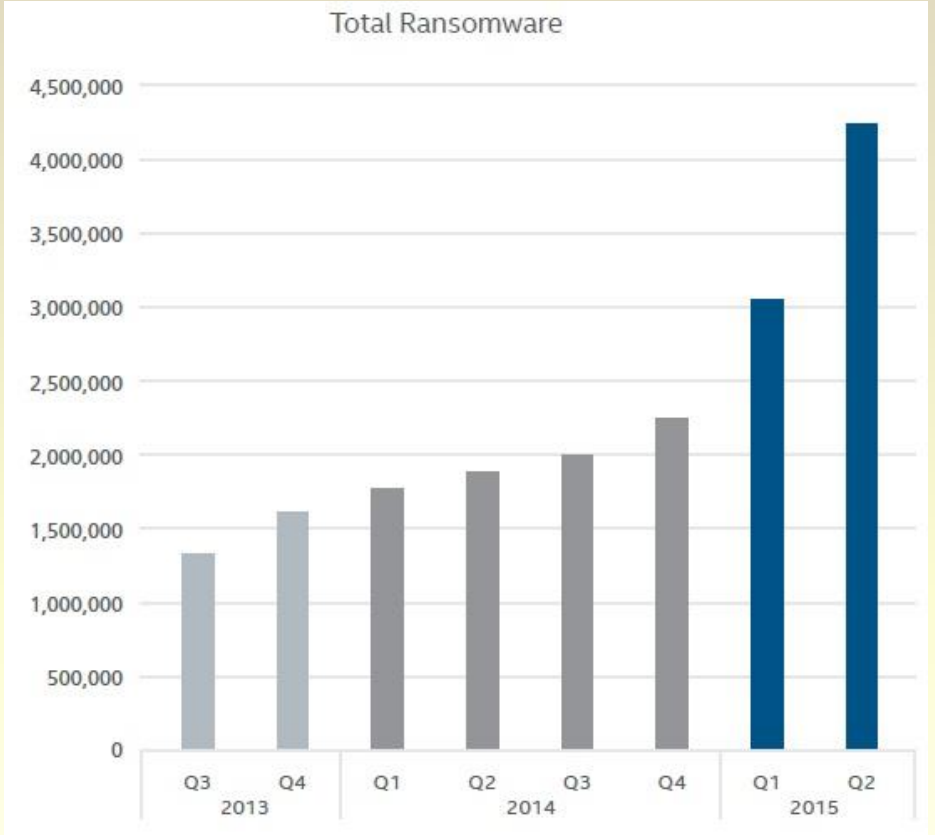




گزارش امنیتی شرکت مک‌آفی در نیمه اول سال ۲۰۱۵

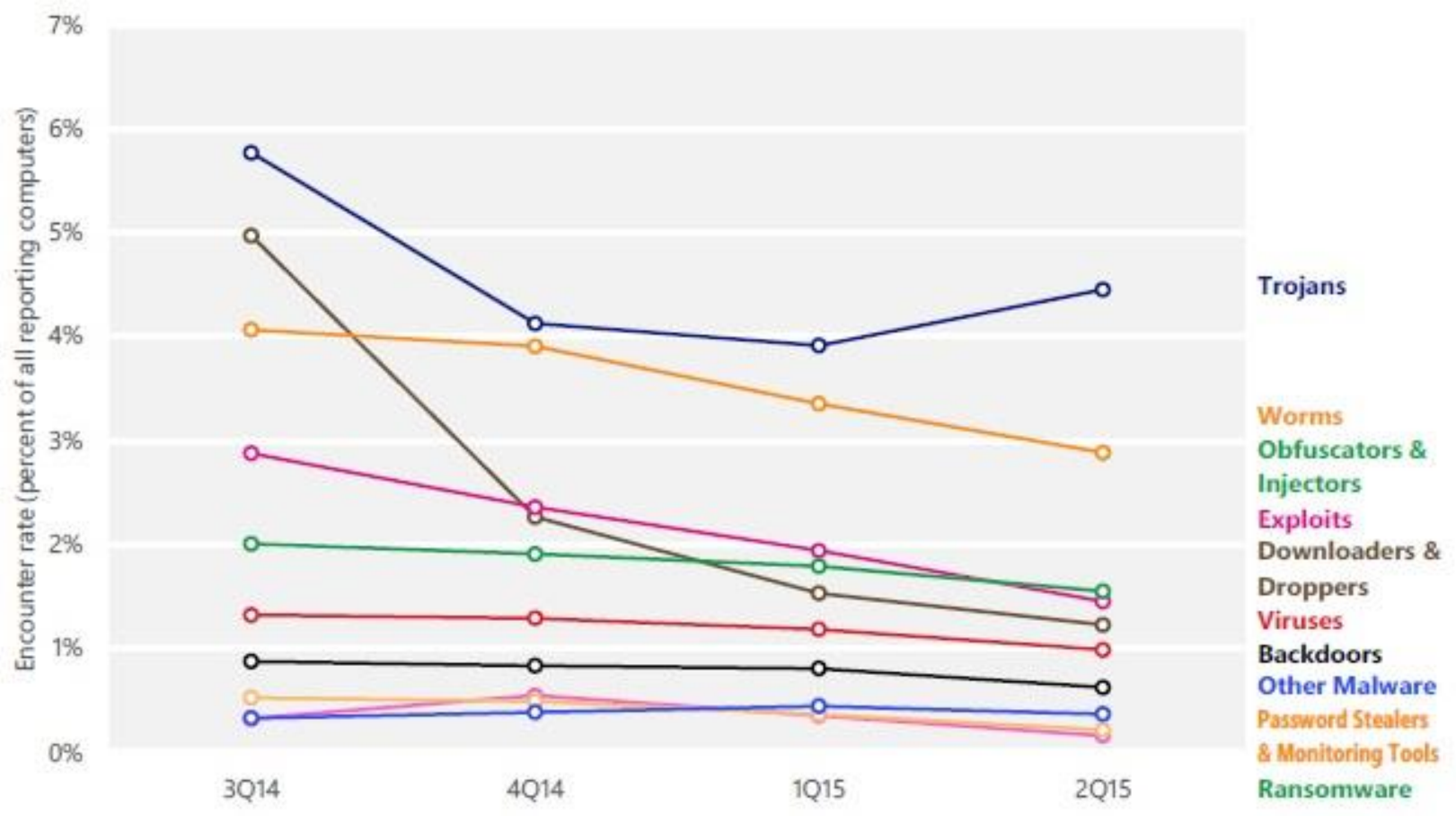
- تعداد بدافزارهای گروگان‌گیر در سه ماهه دوم سال ۲۰۱۵، ۵۸ درصد افزایش یافته است.





گزارش امنیتی شرکت مایکروسافت ۲۰۱۵-۲۰۱٤

- طبقه‌بندی تهدیدات



تهدیدهای امنیتی در گوشی‌های هوشمند و تبلت‌ها

- **شرکت Bitg بیش از ۴۰۰ هزار اپلیکیشن را در گوگل پلی مورد ارزیابی قرار داده است:**

- ۷۲ درصد از تمام اپلیکیشن‌های اندروید یعنی حدود ۲۹۰ هزار برنامه، دست‌کم به یک اجازه نامه بسیار خطرناک دسترسی دارند.
- ۲۱ درصد (بیش از ۸۶ هزار برنامه) به بیش از ۵ مورد پرمیشن خطرناک یا بیشتر دسترسی دارند.
- ۲ درصد یعنی بیش از ۸ هزار اپلیکیشن به ۱۰ مورد اجازه نامه یا بیشتر دسترسی دارند که خطرناک هستند

تعداد نرم‌افزارهای موجود در گوگل پلی و دیگر ارائه‌دهندگان بسیار بیشتر از این عدد است

تهدیدهای امنیتی در گوشی‌های هوشمند و تبلت‌ها

- **طبق گزارش شرکت Bitg :**
  - بسیاری از اپلیکیشن ها سطح دسترسی‌هایی را تقاضا می‌کنند که به قابلیت‌های آن‌ها ارتباطی ندارد.
  - تعداد قابل توجهی از برنامه‌ها عنوان «شناخته شده» دارند. به طور مثال، از ۱۱۵ اپلیکیشنی که دو کلمه Angry و Birds را در عنوان خود دارند، فقط ۴ اپلیکیشن هستند که به کمپانی Rovio Mobile تولیدکننده رسمی اپلیکیشن Angry Birds تعلق دارند. در میان آن‌ها، Angry Birds Live Wallpaper دو برابر بیشتر از برنامه اصلی بازی پرندگان خشمگین تقاضای دسترسی به سیستم کاربر را دارد. به طور مثال، این برنامه تقاضای دسترسی به اطلاعات جی‌پی‌اس را دارد که هیچ ارتباطی به کاربردش ندارد.

گزارش سالانه امنیتی شرکت سیسکو – ۲۰۱۵

- کاربران فقط هدف نیستند بلکه همدستی توانا برای فراهم کردن ایجاد یک حمله به حساب می‌آیند.
- مهاجمین در استفاده از رخنه‌های امنیتی جهت پنهان‌سازی فعالیت‌های مخرب خود ماهرتر شده‌اند.
- حجم هرزنامه‌ها از ژانویه تا نوامبر ۲۰۱٤ میلادی، ۲۵۰ درصد افزایش داشته است.
- سازندگان بدافزارها از افزونه‌های مرورگرها به‌عنوان یک ابزار جهت توزیع بدافزارها و برنامه‌های ناخواسته استفاده می‌کنند.
- اکنون زمانی است که سازمان‌ها باید به‌طور متفاوتی به روند امنیت بنگرند تا بتوانند به‌صورت واقعی سازمان‌هایشان را بیشتر امن سازند.

امنیت در فضای مجازی

تهدیدها، اهداف حملات، لایه‌های امینت، ابزارها و سیاست‌ها

دفاع در عمق

- **استفاده از رویکرد لایه‌ای**
  - افزایش ریسک شناسایی‌شدن برای هکر
  - کاهش احتمال موفقیت هکر

ACL, encryption

Application hardening, antivirus

OS hardening, update management, authentication

Network segments, IPSec, NIDS

Firewalls, VPN quarantine

Guards, locks, tracking devices, HSM

User education against social engineering

تهدیدهای کلی فضای مجازی

- تخریب و انهدام
- تحریف و انحراف
- ربایش و ازاله
- افشا
- قطع و وقفه

اهداف حملات سایبری

- **اهداف سیاسی**
  - تضعیف دولت‌ها (با حمله سایبری به زیرساخت‌های حساس و حیاتی)
- **اهداف اقتصادی**
  - ضربه زدن به رقبا
  - کسب اطلاعات رقبا
  - کسب درآمد از طرق نامشروع
- **اهداف شخصی**
  - انتقام‌جویی (خصومت‌های شخصی یا نارضایتی کاری)
  - اثبات و بروز توانمندی‌ها

لایه‌های امنیت فضای تبادل اطلاعات

- امنیت شخصی
- امنیت فیزیکی
- امنیت اطلاعات
- امنیت عملیات
- امنیت شبکه
- امنیت ارتباطات

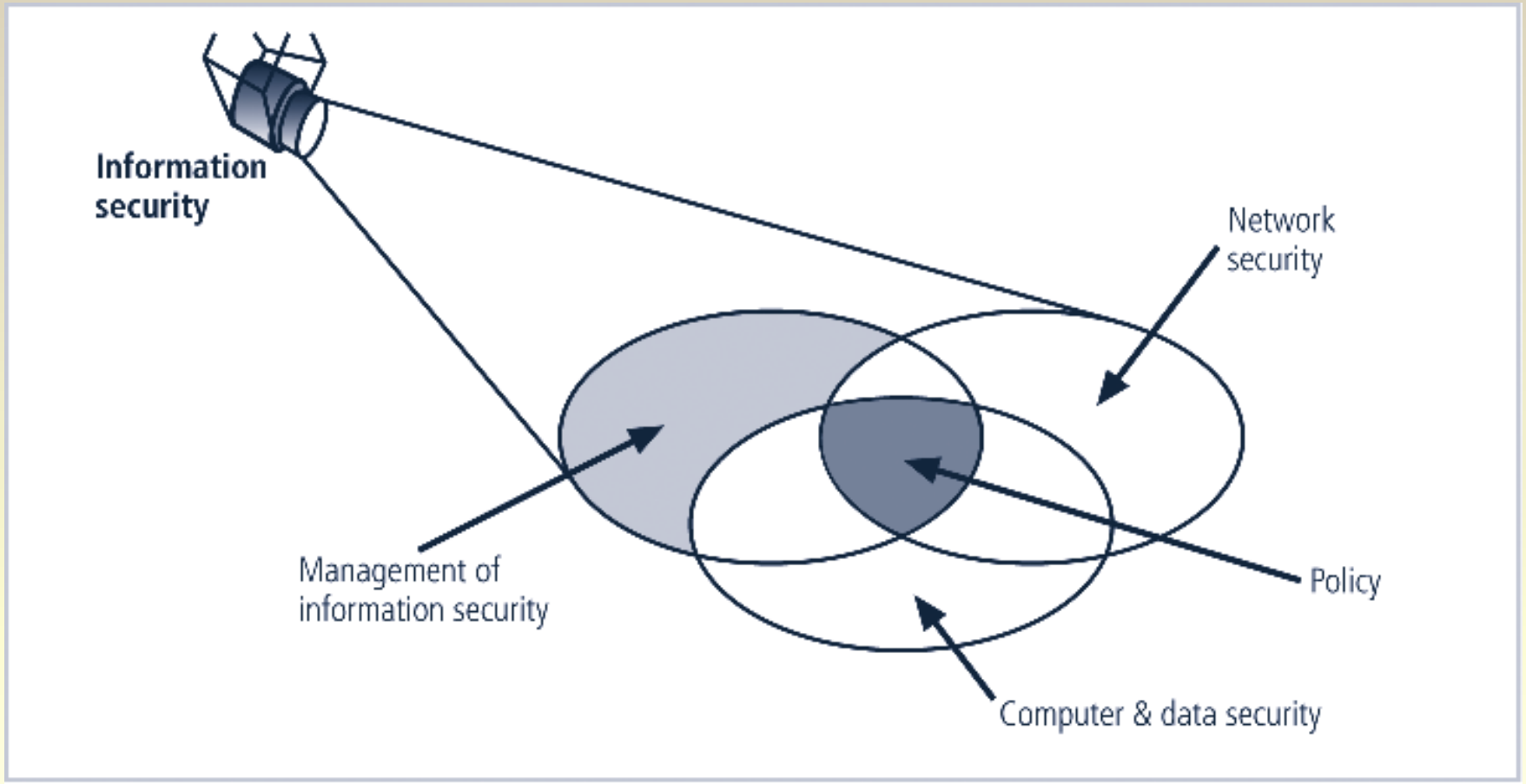
ابزارهای تحقق امنیت فناوری اطلاعات

- سیاست
- آگاهی
- آموزش
- فناوری

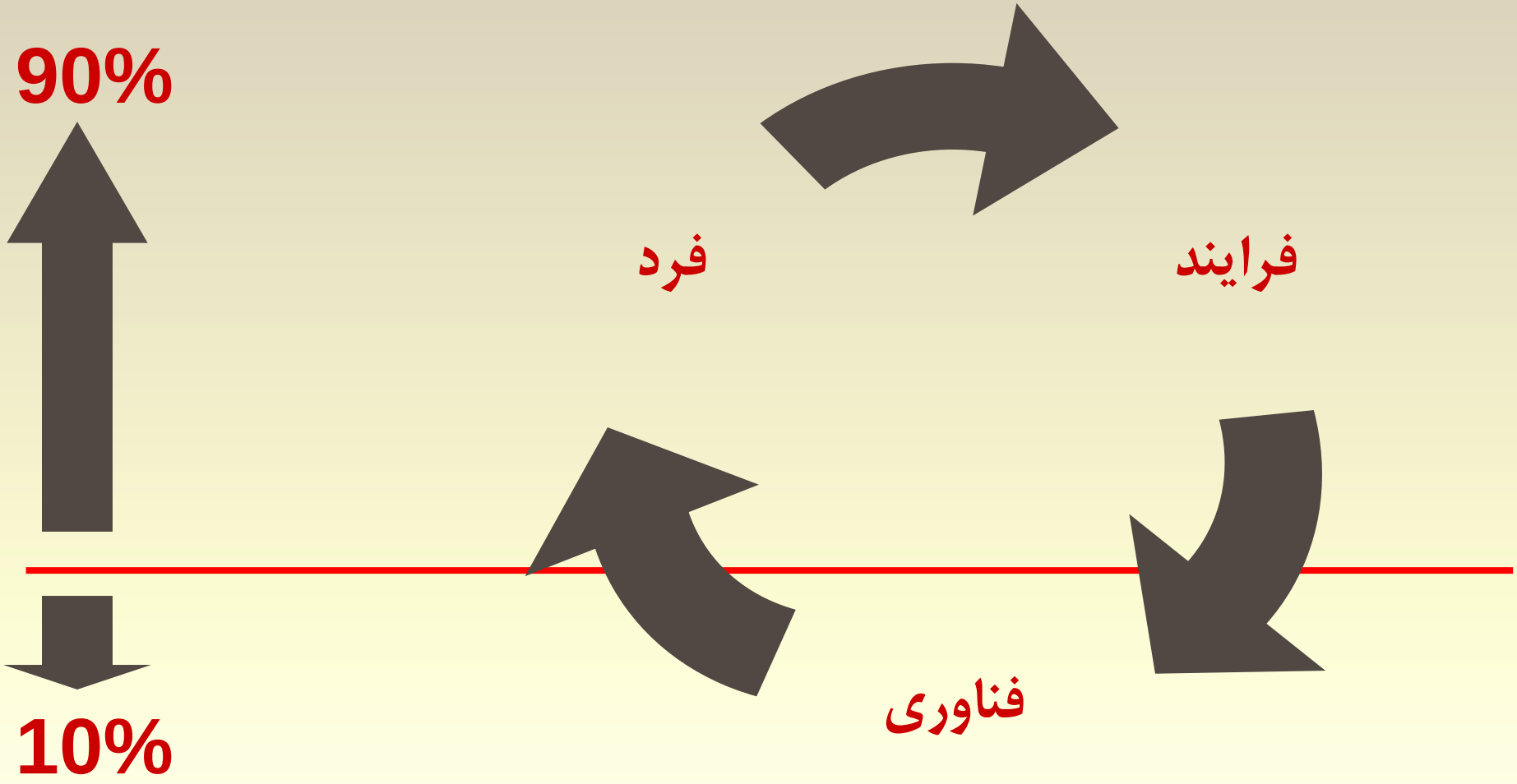
توازن در برقراری امنیت فضای تبادل اطلاعات

- توازن امنیت اطلاعات و دسترسی
- دست‌یافتن به سطح کامل امنیت در فناوری اطلاعات و ارتباطات ممکن نیست.
- برای برقراری سطح مطلوب امنیت اطلاعات باید تعادل مناسب بین حفاظت و دسترسی‌ها ایجاد شود.

امنیت فضای تبادل اطلاعات



امنیت فضای تبادل اطلاعات



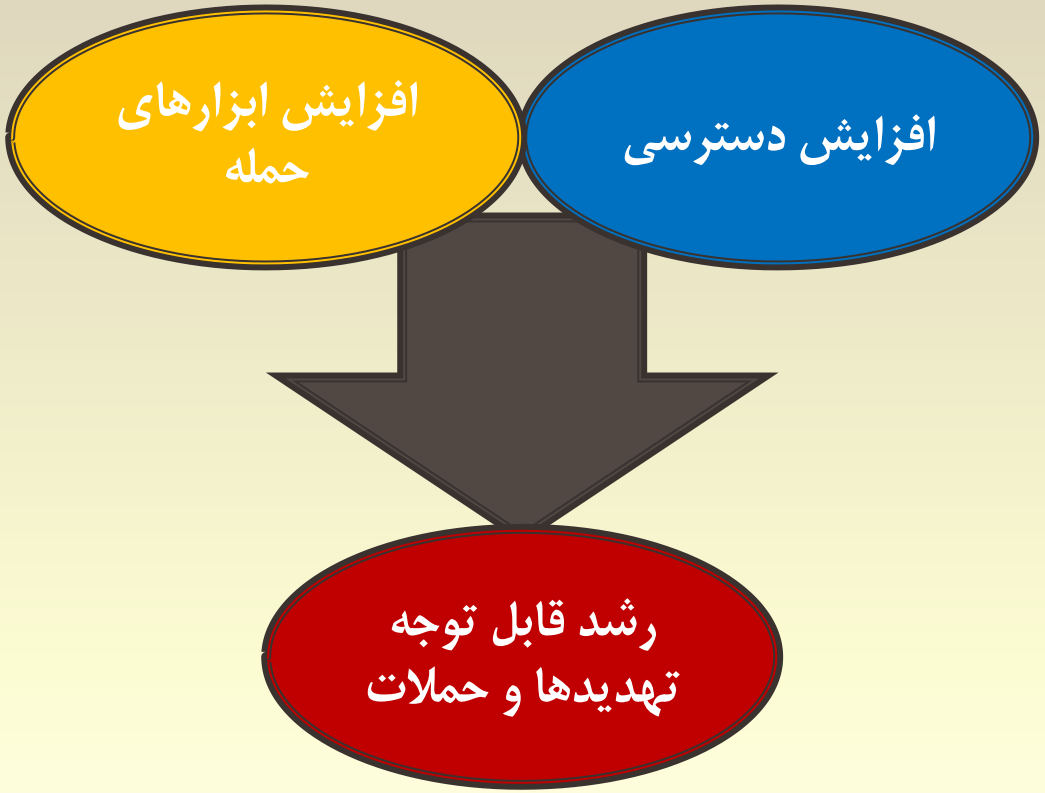
نقش کاربران در امنیت فضای تبادل اطلاعات

- در امنیت اطلاعات؛ بزرگ‌ترین دارایی افراد هستند و بزرگ‌ترین تهدید نیز افراد می‌باشند.

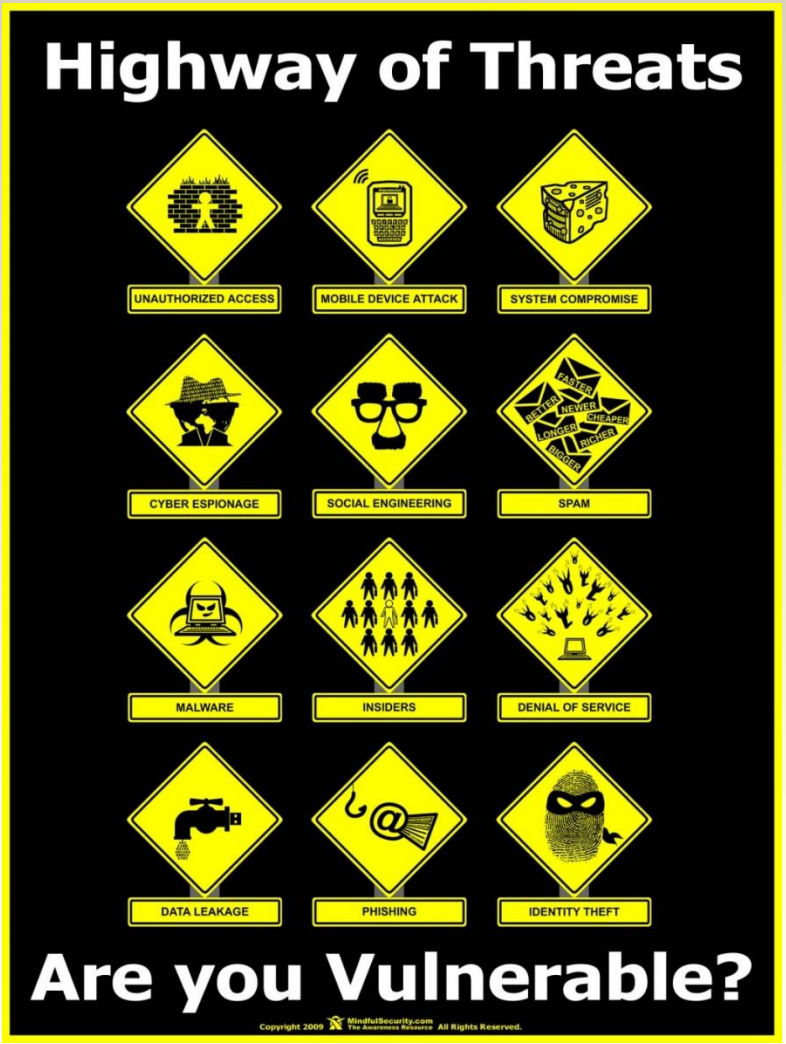
روندهای امنیت فناوری اطلاعات و ارتباطات

روندهای تهدیدها و حملات

رشد تهدیدها و حملات در فضای مجازی



تهدیدهای فضای تبادل اطلاعات



منشا خطاهای احتمالی در کاربری

- خطاهای ناشی از نبود دانش
- خطاهای ناشی از نبود تجربه
- خطاهای ناشی از آموزش نادرست
- خطاهای ناشی از پیش‌فرض‌های نادرست

در فضای مجازی، آن چه می‌بینید، تمام واقعیت نیست

ساده‌شدن حملات

شبکه‌های اجتماعی؛ فرصت و تهدید

روندهای امنیت فناوری اطلاعات و ارتباطات

- اینترنت اشیا (IoT) ؛ ملاحظات امنیتی، حقوقی و غیره
- تدوین مقررات حفاظت از اطلاعات در اروپا
  - افزایش حملات هدفمند به سازمان‌ها و شرکت‌ها به منظور سرقت اطلاعات
  - با اعمال این مقررات از سال ۲۰۱۷، مسوولیت سازمان‌ها و شرکت‌ها در قبال امنیت اطلاعات افزایش می‌یابد.

روندهای امنیت فناوری اطلاعات و ارتباطات

- **تمرکز نفوذگران به تلفن‌های هوشمند، رایانه‌های همراه و . . .**
  - با توجه به مخاطرات این حوزه، سازمان‌ها و شرکت‌ها، رویکرد کارمندمحوری را در زمینه امنیت اطلاعات برگزیده‌اند.
- **شکاف عمیق در دانش و مهارت جهانی در حوزه امنیت**

روندهای امنیت فناوری اطلاعات و ارتباطات

- امنیت در سامانه‌های کنترل صنعتی

- تمرکز بر سیاست‌های پاسخ به حملات در کنار سیاست‌های پیش‌گیرانه

روندهای امنیت فناوری اطلاعات و ارتباطات

- **امینت سامانه‌های پردازش ابری**

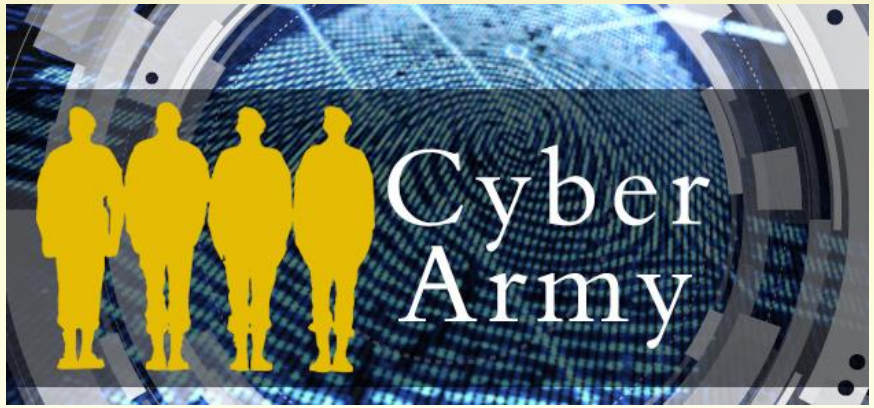
- **داده‌های بزرگ؛ الزامات امنیتی در نرم‌افزارها و کاربردها**
  - نگرانی از امنیت داده‌ها در سال ۲۰۱۵ تاثیر منفی در نوآوری برخی سازمان‌ها و شرکت‌ها داشته است.

روندهای امنیت فناوری اطلاعات و ارتباطات

- تغییرات و ارتقای شبکه‌های اجتماعی
- نرم‌افزارهای پیام‌رسان، نسل جدید شبکه‌های اجتماعی

روندهای امنیت فناوری اطلاعات و ارتباطات

- ادامه افزایش حملات بدافزارهای گروگان‌گیر



- ادامه تلاش دولت‌ها در انجام حملات سایبری و ...

روندهای امنیت فناوری اطلاعات و ارتباطات

افزایش روند BYOD ها و نگرانی از امنیت آن‌ها

- بر اساس آمارگیری از ۱۱۵۰۰ کارمند در ۲۳ کشور مشخص شده است که ۸۷ درصد آن‌ها گمان می‌کردند بخش فناوری اطلاعات و ارتباطات از آن‌ها در برابر تهدیدات محافظت می‌کنند.
- ۳۱ درصد اذعان کرده‌اند که داده‌های آن‌ها در تلفن همراهشان را از دست داده‌اند.

روندهای امنیت فناوری اطلاعات و ارتباطات

- **چالش های امنیتی در شبکه‌های نظارت تصویری**
- یک شبکه کاملاً امنیتی با اهداف خاص
- گزارش‌ها و بازدیدهای فنی نشان داده است که این نوع شبکه‌ها از دانش فنی و نگرش امنیتی مناسبی در فرآیندهای زیر برخوردار نیستند:
  - طراحی شبکه و زیرساخت
  - پیکربندی و مدیریت
- القاء حس کاذب امنیت در این شبکه ها به دلیل:
  - جداسازی از شبکه مرسوم سازمانی!!
  - غفلت از سایر مولفه‌های امنیتی
  - عدم کارایی و قابلیت اطمینان در این نوع شبکه‌ها

ضرورت‌های امنیت فناوری اطلاعات و ارتباطات

راهکارها

نقاط ضعف در کاربست امنیت فناوری اطلاعات و ارتباطات

- **ضعف فناوری**
  - پروتکل، سیستم عامل، تجهیزات
- **ضعف تنظیمات**
  - رهاکردن تنظیمات پیش‌فرض، گذرواژه‌های نامناسب، عدم استفاده از رمزنگاری، راه‌اندازی سرویس‌های اینترنت بدون اعمال تنظیمات لازم، ...
- **ضعف سیاست‌گذاری**
  - عدم وجود سیاست امنیتی
  - عدم وجود طرحی برای مقابله و بازیابی مخاطرات
  - نداشتن نظارت امنیتی مناسب (مدیریتی و فنی)
- **ضعف دانش و آگاهی**
  - عدم اطلاع از تنظیمات حریم خصوصی، نبود دانش کافی برای استفاده امن از شبکه‌های اجتماعی

امنیت فناوری اطلاعات و ارتباطات؛ بایدها و نبایدها

- نگرش جامع به مسالهٔ امنیت لازم است و نه فقط نگرش فنی و مقطعی.
- امن‌سازی به مراتب سخت‌تر از ناامن‌سازی است.
- امن‌سازی یک فرایند است (نه یک محصول و وظیفه خاص و مقطعی).
- امن‌سازی سیستم مستلزم سرمایه‌گذاری‌های جدی و زمان‌بر است.
- مادام که انسان‌ها امن فکر نکنند نمی‌توان سیستم امن داشت.

اصول اولیه امنیت (بیانیه امنیتی سیسکو)

- **امنیت باید موتور رشد شرکت در نظر گرفته شود.**
  - امنیت هیچ‌گاه نباید مانع بازده و نوآوری شرکت شود.
- **امنیت باید با معماری موجود کار کند و قابل استفاده باشد.**
  - سازمان‌های برای اینکه با فناوری امنیت خود را سازگار کنند، نباید روش‌های کسب و کار خود را تغییر دهند.
- **امنیت باید شفاف و آموزنده باشد.**
  - کاربران باید اطلاعاتی در اختیارشان قرار داده شود که بفهمند چرا مسائل امنیتی مانع از انجام برخی اعمال می‌شود.
- **امنیت باید قابلیت رؤیت باشد و انجام عمل مناسب را ممکن کند.**
  - راه‌حل‌های امنیتی که دارای معماری امنیتی باز هستند تیم‌های امنیتی را قادر می‌سازند که بفهمند آیا این راه‌حل‌ها واقعاً مؤثر هستند.
- **امنیت باید به عنوان راه حلی برای مردم در نظر گرفته شود.**
  - هنگام مواجه شدن با مسائل امنیتی اتخاذ روشی که تمرکزش بر روی فناوری است امنیت را بهبود نمی‌بخشد؛ بلکه آن را بدتر می‌کند.

چرخه ایجاد امنیت

سرویس‌های امن‌سازی

آزمایشگاه تخصصی آپا دانشگاه فردوسی مشهد

معرفی خدمات و فعالیت‌ها

حوزه فعالیت‌ها

- **رسیدگی به حوادث:** دریافت، تحلیل و پاسخ به حوادث رایانه‌ای و رخدادهای امنیتی
- **رسیدگی به آسیب‌پذیری‌ها:** دریافت اطلاعات لازم در مورد وجود آسیب‌پذیری‌ها در شبکه‌های رایانه‌ای و سامانه‌های نرم‌افزاری، تحلیل ماهیت و اثرات آن‌ها
- **اطلاع‌رسانی:** گزارش آسیب‌پذیری‌ها و ارائه هشدارهای امنیتی
- **آموزش:** گسترش دانش در زمینه امنیت فناوری اطلاعات و ارتباطات
- **مشاوره امنیتی:** ارائه توصیه‌ها، راهنمایی‌ها و مشاوره‌های امنیتی به متقاضیان
- **آزمون نفوذپذیری:** ارزیابی امنیت شبکه‌های رایانه‌ای و سامانه‌های نرم‌افزاری برای کشف آسیب‌پذیری‌های بالقوه و ارائه راه‌کارهای رفع آن‌ها

خدمات

- **آزمون نفوذپذیری**
  - شبکه‌های رایانه‌ای
  - برنامه‌های کاربردی تحت وب
  - پورتال‌ها
  - سامانه‌های نظارت تصویری
- **تدوین طرح امنیت جامع شبکه‌های رایانه‌ای**
- **صدور گواهینامه امنیتی برای نرم‌افزارهای کاربردی تحت وب**
  - OWASP ASVS 1A certificate
- **برگزاری دوره‌های آموزشی تخصصی به صورت حضوری و مجازی**
- **فعالیت‌های پژوهشی و تحقیقاتی**
- **انتشار دانش**

دستاوردها

- نهادینه‌سازی افتا و نظام آپا در مدیریت کلان استان خراسان رضوی
- آشنایی مدیران کلان و مدیران فناوری اطلاعات سازمان‌های اجرایی استان خراسان رضوی با اهمیت افتا و کارکرد آپا
- افزایش اهمیت امنیت اطلاعات در بین شرکت‌های ارائه‌دهنده خدمات سخت‌افزاری و نرم‌افزاری و خدمات آپا به این شرکت‌ها
- آگاه‌نمودن بخشی از کارشناسان سازمان‌های اجرایی با اهمیت افتا
- ایجاد انگیزه برای دانشجویان مهندسی کامپیوتر برای انتخاب گرایش‌های مرتبط با امنیت و ادامه تحصیل در این گرایش
- دعوت از آزمایشگاه تخصصی آپا دانشگاه فردوسی مشهد برای حضور در نمایشگاه‌های تخصصی فاوا و ارائه سمینارهای آموزشی مرتبط در آن‌ها

کسب رتبه از سومین جشنواره فناوری اطلاعات و ارتباطات

سومین جشنواره ملی ارتباطات و فناوری اطلاعات

امنیت، سرعت و کاهش هزینه ها با شبکه ملی اطلاعات

به نام آفریننده کهکشان و آگاهی

توسعه و تکامل پرجاذبه و فراگیر ارتباطات کشور در عصر جامعه ی دانش بنیان و بهره مندی از فناوری اطلاعات و ژرفای ارزشمندترین دستاوردهای اقتدار نظام مقدس جمهوری اسلامی در عرصه های بین المللی است و ولی تنگ این آسمان شرنگ تنها پرتو تلاش و دست اندرکاران، متخصصان، مدیران و دگر دست اندرکاران این حوزه تحقق یافتنی ست.

آزمایشگاه تخصصی آپا دانشگاه فردوسی مشهد

اکنون که در دهه ی پیشرفت و عدالت و در سال حماسه ی سیاسی، حماسه ی اقتصادی

در سومین جشنواره ملی ارتباطات و فناوری اطلاعات (یادواره ی شهید دکتر قندی)

حائز کسب رتبه دوم در کارگروه امنیت فضای تبادل اطلاعات محور مراکز آموزشی و تحقیقاتی شده اید؛

به نشانه ی قدردانی و به پاس ارج نهادن به تلاش های گرانسنگ تان

این لوح سپاس اهداء می شود.

عزت ، سربلندی، سرافرازی و سرزندگی تمامی تلاشگران حوزه ارتباطات کشور در پناه حضرت دوست

و عنایت خاصه ی حضرت بقیه الله الاعظم (عج) و تحت زعامت ولی امر مسلمین جهان حضرت

آیت الله العظمی خامنه ای (مدظله العالی)، مستدام و پاینده باد.

محمد حسن نامی

وزیر ارتباطات و فناوری اطلاعات

برخی سازمان‌ها و دستگاه‌های که تاکنون با آن‌ها قرارداد منعقد شده است

- استانداری خراسان رضوی
- استانداری خراسان شمالی
- سازمان فناوری اطلاعات ایران – مرکز ماهر
- اداره اطلاعات خراسان رضوی
- شهرداری تهران
- مرکز پدافند سایبری کشور
- اداره‌کل گمرکات استان خراسان رضوی
- اداره‌کل نوسازی، توسعه و تجهیز مدارس خراسان رضوی
- اداره‌کل تنظیم مقررات و ارتباطات رادیویی شمال شرق
- شرکت آب و فاضلاب شهری خراسان شمالی
- اداره کل هواشناسی خراسان رضوی
- شرکت توزیع نیروی برق خراسان رضوی
- شرکت توزیع نیروی برق مشهد
- آستان قدس رضوی
- موسسه فرهنگی هنری خراسان
- سازمان صنعت، معدن و تجارت استان خراسان رضوی
- و بیش از ۲۰ شرکت و سازمان خصوصی

گزارش آماری عملکرد

- ارزیابی امنیتی و آزمون نفوذپذیری برنامه های کاربردی تحت وب
  - بیش از ۱۵۰ مورد
- ارزیابی امنیتی و آزمون نفوذپذیری شبکه ها و زیرساخت
  - بیش از ۵۰ مورد
- ارائه گواهی های امنیتی برنامه کاربردی تحت وب
  - ۱۲ مورد
- ارائه مشاوره های تخصصی، ارائه طرح جامع شبکه و امنیت و استقرار
  - بیش از ۱۰ مورد
- برگزاری دوره های آموزشی و تخصصی مرتبط
  - بیش از ۵۰ دوره – بیش از ۱۵۰۰ ساعت

گواهی‌نامه امنیتی برنامه‌های کاربردی تحت وب

گواهی‌نامه

CERTIFICATE

گواهی‌نامه امنیت برنامه‌های کاربردی تحت وب

گواهی می‌شود برنامه کاربردی تحت وب [redacted] با مشخصات فنی پیوست، پس از نصب بر روی سرویس‌دهندگان آزمایشگاه تخصصی آپا دانشگاه فردوسی مشهد و بر اساس تنظیمات انجام شده مورد ارزیابی امنیتی قرار گرفت و در تاریخ ۱۳۹٤/٤/۱۵ موفق به دریافت گواهی‌نامه امنیت برنامه‌های کاربردی تحت وب آزمایشگاه تخصصی آپا دانشگاه فردوسی مشهد شد.

این گواهی‌نامه بنا به درخواست [redacted] و برای نسخه موجود در آزمایشگاه تخصصی آپا صادر شده است. بدیهی است اعمال هرگونه تغییر در کد برنامه و تنظیمات انجام شده نیازمند دریافت گواهی‌نامه جدید است. اشخاص حقیقی و حقوقی متقاضی استفاده از این برنامه کاربردی به منظور کنترل صحت گواهی‌نامه می‌توانند کد درج شده ذیل را در وب‌گاه آزمایشگاه تخصصی آپا دانشگاه فردوسی مشهد به نشانی http://cert.um.ac.ir/certificate جستجو نمایند.

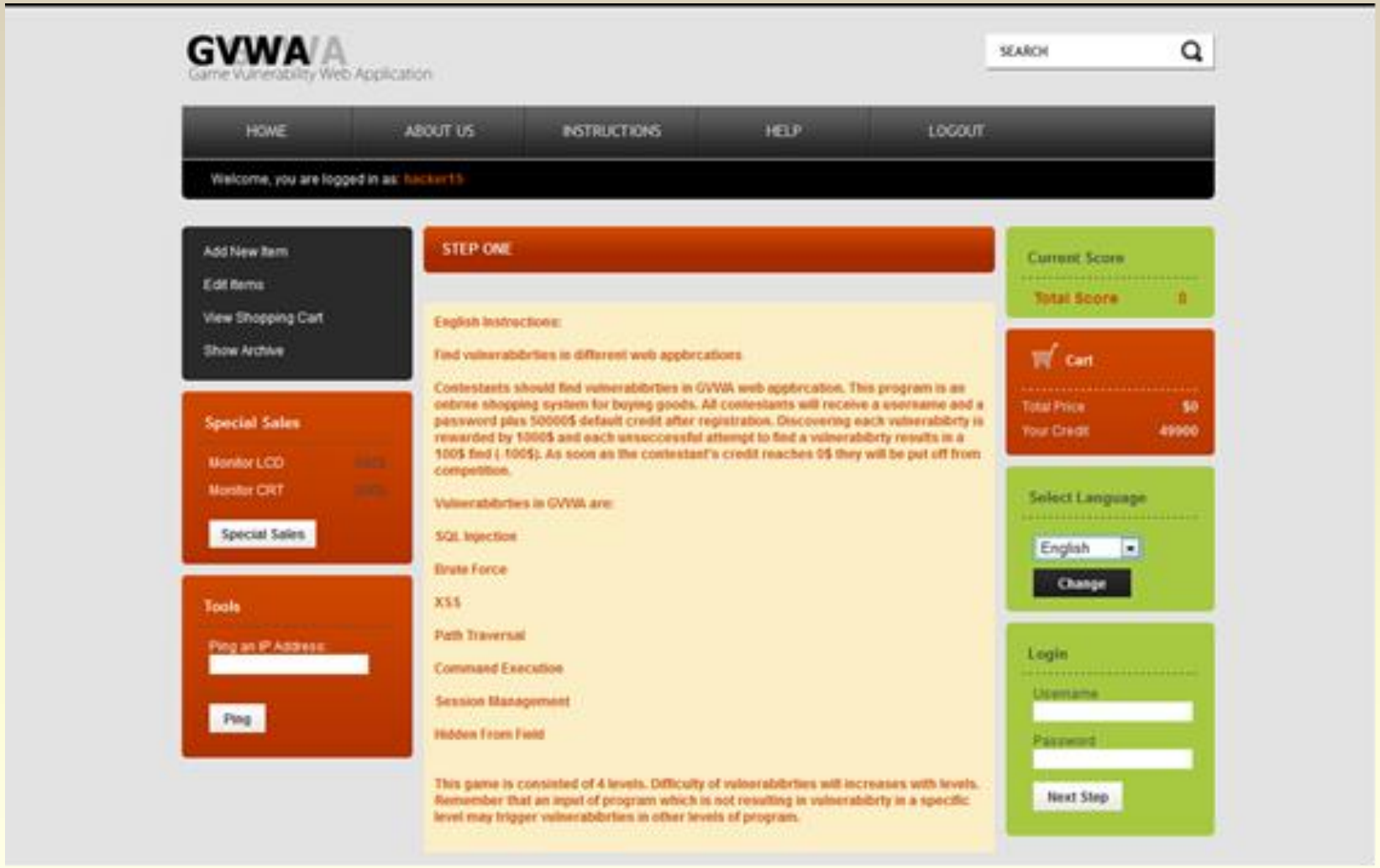
کد گواهی‌نامه : [redacted]

دکتر محسن کاهانی

مدیر آزمایشگاه تخصصی آپا دانشگاه فردوسی مشهد

این گواهی‌نامه با شماره ٦۹ در تاریخ ۱۳۹٤/٤/۲٤ در دبیرخانه آزمایشگاه تخصصی آپا دانشگاه فردوسی مشهد ثبت شده است و با امضا و مهر برجسته آزمایشگاه معتبر می‌باشد.

طراحی و پیاده‌سازی برنامه کاربردی آزمون کشف آسیب‌پذیری در برنامه کاربردی تحت وب



وب‌گاه آزمایشگاه تخصصی آپا دانشگاه فردوسی مشهد

سامانه ویکی آزمایشگاه تخصصی آپا دانشگاه فردوسی مشهد

سامانه SOC آزمایشگاه تخصصی آپا دانشگاه فردوسی مشهد

دوره آموزش مجازی آگاهی‌های امنیتی شبکه‌های رایانه‌ای

از بذل توجهتان متشکرم

http://cert.um.ac.ir

tayarani@um.ac.ir