ریاست جمهوری
سازمان مدیریت و برنامه ریزی
مرکز آموزش و پژوهش

امنیت کاربری فناوری اطلاعات (اکفا)

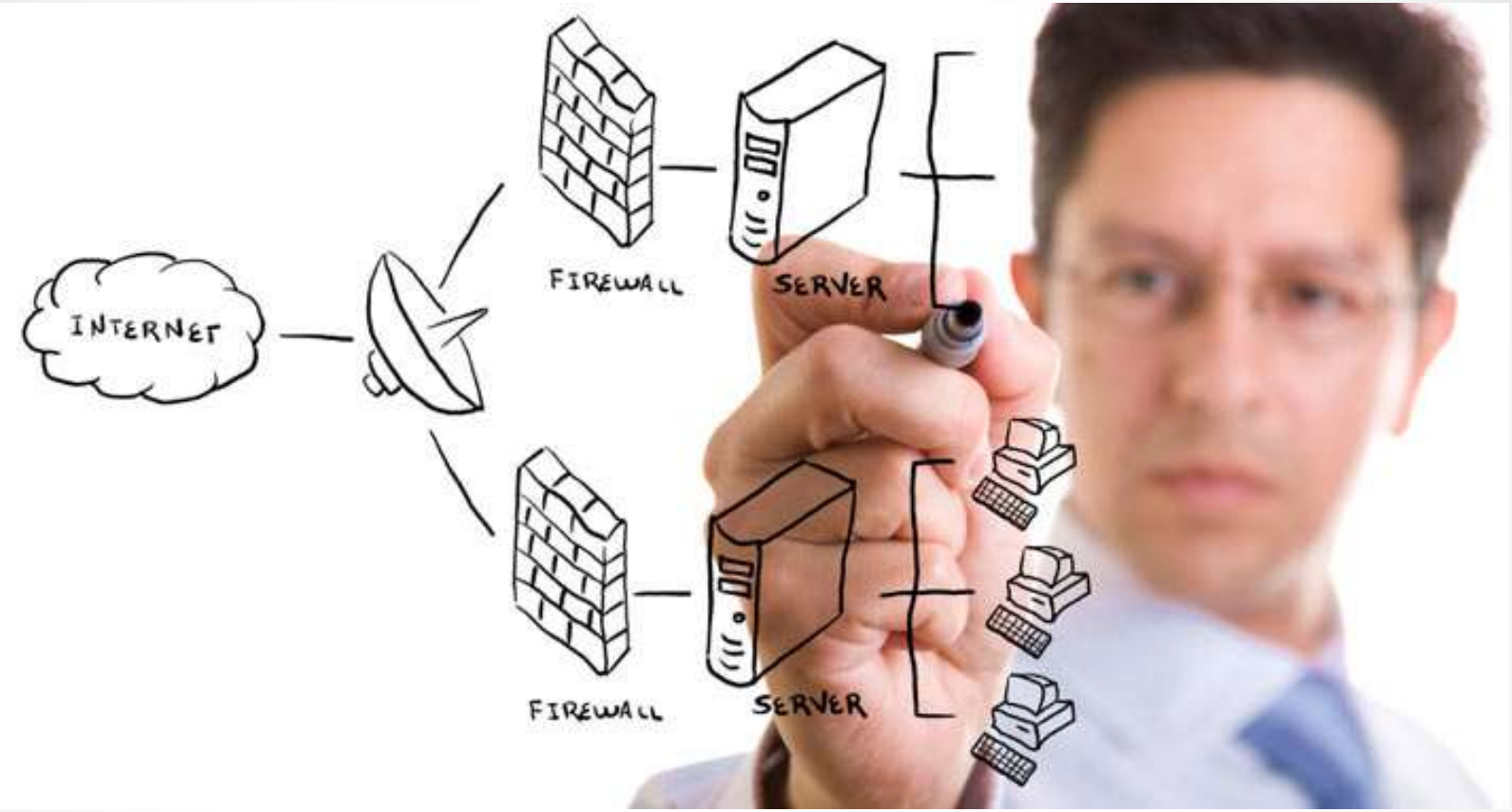
مدرس: مهدی هدایت فر

جلسه اول
مفاهیم امنیت سایبری

جلسه دوم
بهداشت سایبری و مفاهیم حقوقی

جلسه سوم
روشهای کنترل و مقابله

جلسه چهارم
نهادهای متولی و کار عملی



جایگاه امنیت اطلاعات

تعریف امنیت

اَمنیّت حالت فراغت نسبی از تهدید یا حمله یا آمادگی برای رویارویی با هر تهدید و حمله را گویند. امنیت از ضروری‌ترین نیازهای یک جامعه **است.**

دانشنامه سیاسی- داریوش آشوری-نشر مروارید- چاپ شانزدهم ۱۳۸۷- ص۳۸

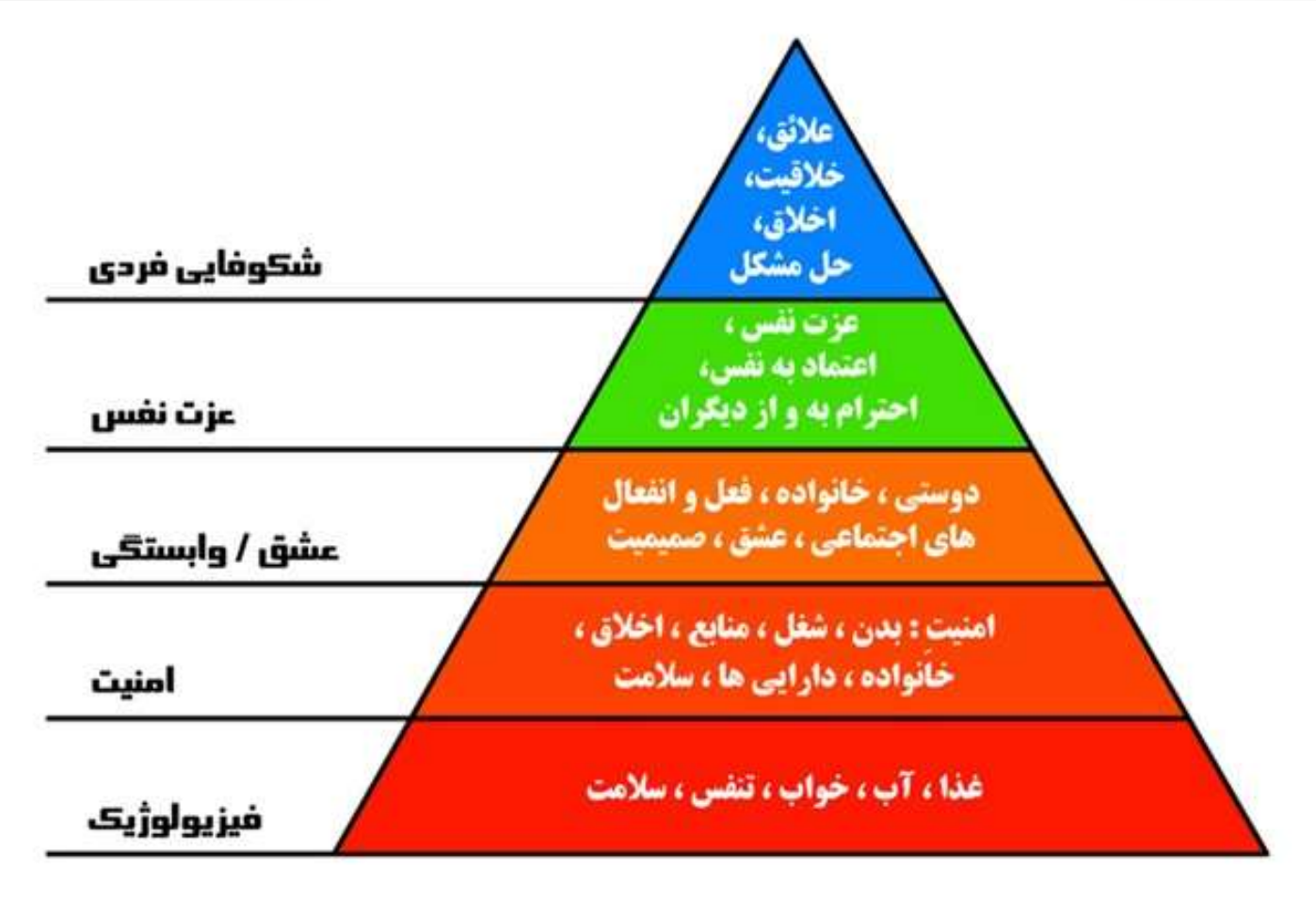
امنیت=به فارسی برابر زنهار است

لغت نامه دهخدا

از هر طرف که رفتم جز وحشتم نیفزود
زنهار از این بیابان وین راه بی‌نهایت

حافظ

سلسله مراتب نیازهای مازلو



انواع امنیت

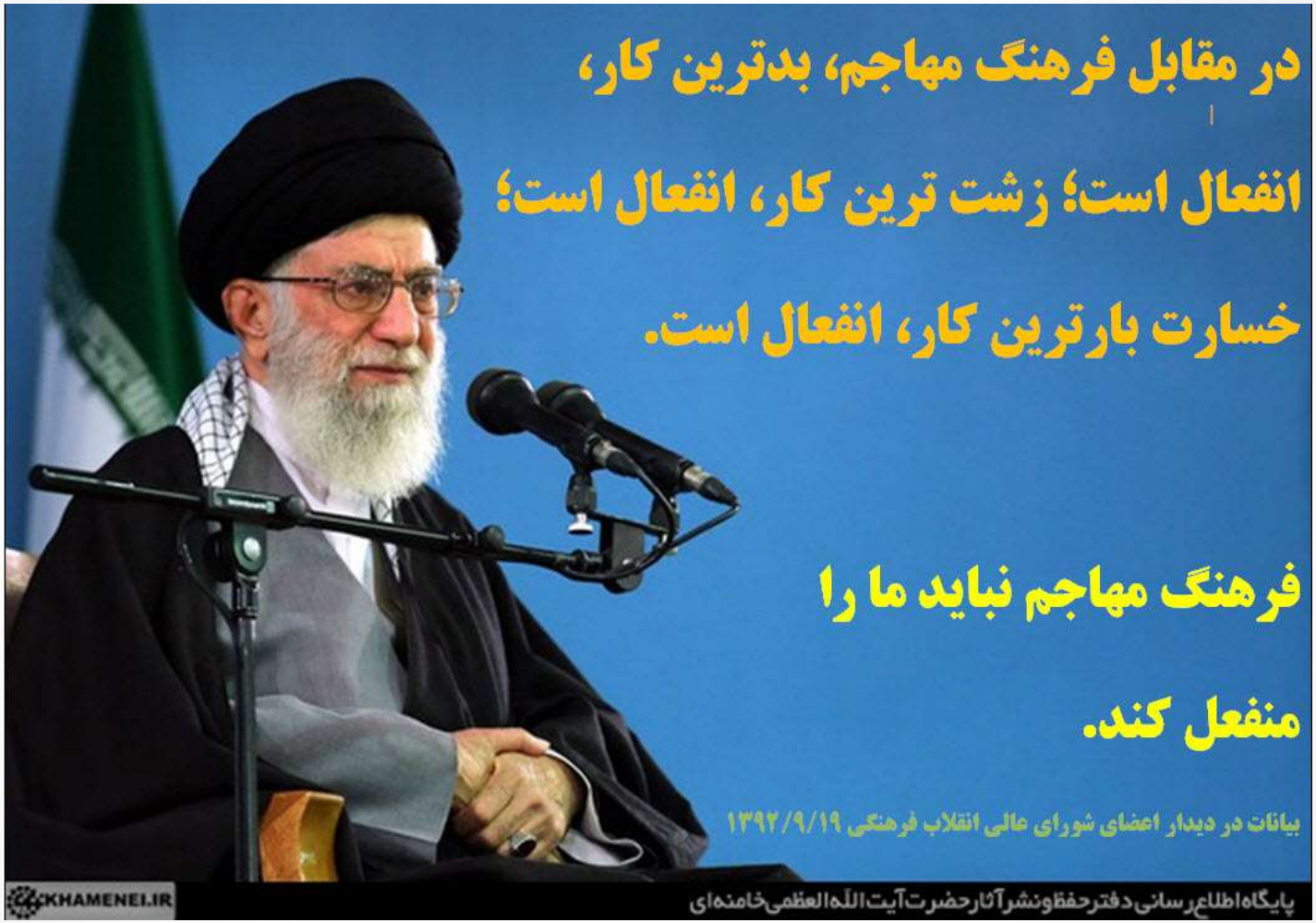
امنیت به لحاظ گستره تاثیر:

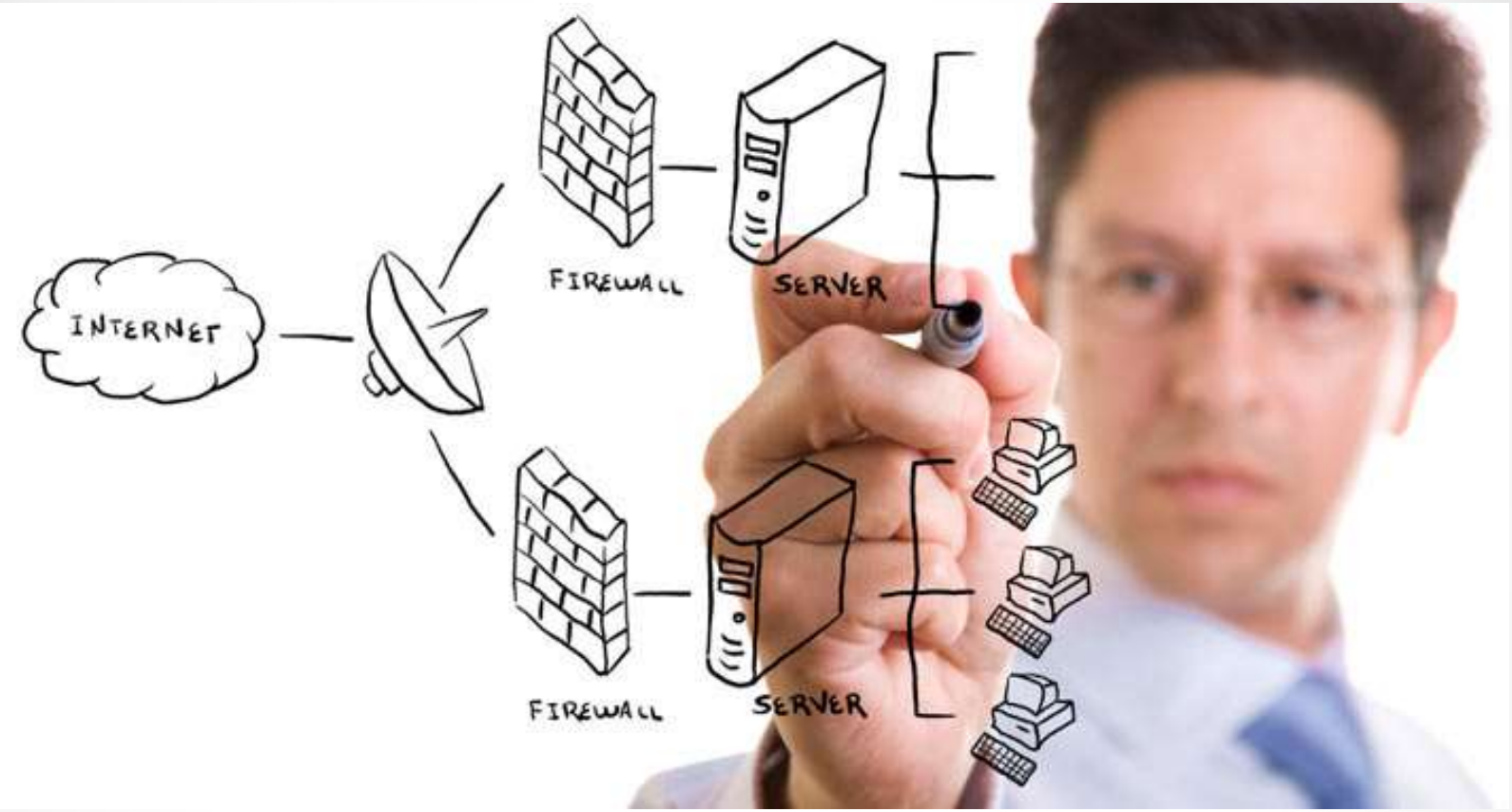
- امنیت فردی
- امنیت خانواده
- امنیت اجتماعی
- امنیت ملی
- امنیت منطقه ای
- امنیت بین المللی

امنیت به لحاظ موضوع:

- امنیت اقتصادی
- امنیت فرهنگی
- امنیت روانی
- امنیت شهری
- امنیت بهداشتی
- امنیت سایبری


امام خامنه ای :
فضای مجازی به اندازه انقلاب اسلامی اهمیت دارد.
Cyberspace is as important as the Islamic Revolution.
GHASAM.ir
پایگاه مقاومت بسیج شهید منتظری


در مقابل فرهنگ مهاجم، بدترین کار،
انفعال است؛ زشت ترین کار، انفعال است؛
خسارت بارترین کار، انفعال است.
فرهنگ مهاجم نباید ما را
منفعل کند.
بیانات در دیدار اعضای شورای عالی انقلاب فرهنگی ۱۳۹۲/۹/۱۹
KHAMENEI.IR
پایگاه اطلاع رسانی دفتر حفظ و نشر آثار حضرت آیت الله العظمی خامنه ای



واقعیت امنیت اطلاعات

نمونه هک ها


هند
GHOSTNET ، نام حمله
۲۰۰۹-۲۰۰۷ ، تاریخ
سفارتخانه های بسیاری از ، هدف
کشور ها نظیر آمریکا،
دفتر تبعیدیان تبت
نامعلوم،نفوذ به رایانه کاربران ، آسیب
Shadow in the cloud ، نام حمله
۲۰۱۰-۲۰۰۹ ، تاریخ
هدف،دفاتر دولتی هند و تبت،
دفتر سازمان ملل
آسیب ،تبعیدیان تبت و مکاتبات
محرمانه دولت هند به خطر افتاد
آمریکا
AURORA، نام حمله
۲۰۰۹ ، تاریخ
فعالان حقوق بشر چینی ، هدف
پایگاه فناوری مستقر در آمریکا
سرقت رمز عبور کاربران گوگل، آسیب
به خطر افتادن ایمیل فعالان
BYZANTINE CANDOR ، نام حمله
۲۰۰۲-؟ ، تاریخ
هدف،نیروی های نظامی و سازمان های
دولتی آمریکا
آسیب ، سرقت بخش زیادی از اطلاعات حساس
چین
WIKILEAKS TAKE DOWN ، نام حمله
۲۰۱۰ ، تاریخ
علت ، انتشار اسناد محرمانه
آسیب ، قطعی مکرر سایت
غیر فعال کردن دامنه سایت
گرجستان
علت ،جنگ اوستیای جنوبی
تاریخ ، ۲۰۰۸
آسیب ، وب سایت دولت گرجستان
برای چندین ساعت غیر فعال شد
ایران
STUXNET ، نام حمله
۲۰۱۰ - ۲۰۰۹ ، تاریخ
هدف، سیستم های صنعتی
آسیب ، ویروسی شدن چند رایانه، اخلال در فعالیت
نیروگاه هسته ای
رژیم
صهیونیستی
روسیه
پایود جنگ شوروی ، علت
و انتخاب تالین به عنوان پایتخت
۲۰۰۷ ، تاریخ
وب سایت دولت ،بانک ها و روزنامه ها، آسیب
برای چندین ساعت غیر فعال شد

گزارش کسپرسکی

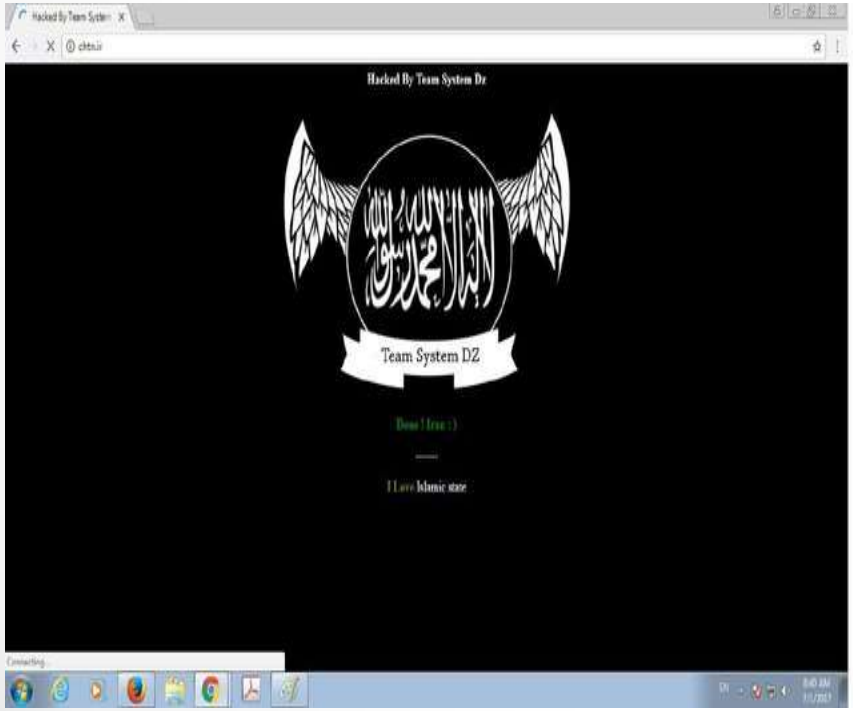
آمار هک در ایران

- روزانه به طور متوسط بالغ بر ۱۰ هزار سانحه امنیتی سایبری
- روزانه هک ۳۶ وبسایت
- ۷۳% حفره های کشف شده در سال ۹۰ مربوط به سایتهای دولتی بوده
- ۶۰% مربوط به بانکهای دولتی
- بیش از ۲۰۰ سایت ایرانی توسط تیم هکر DZ (منتسب به داعش)از دسترس خارج شد

نمونه هک ها

هک سایت وزارت ورزش عربستان توسط ایرانیان

هک سایت های ایرانی توسط داعش



پیامدهای منفی وجود حفره های امنیتی در سازمان

- کاهش درآمد و افزایش هزینه
- خدشه به اعتبار و شهرت یک سازمان
- از دست دادن داده و اطلاعات مهم
- اختلال در فرآیندهای جاری یک سازمان
- پیامدهای قانونی به دلیل عدم ایجاد یک سیستم ایمن و تاثیر جانبی منفی بر فعالیت سایر سازمان ها
- سلب اعتماد مشتریان
- سلب اعتماد سرمایه گذاران

جنگ واقعی سایبری

خونسرد نباشید

دولت بریتابیا که در طول تاریخ در شراط بحرانی همیشه شهروندان خود را « به حفظ آرامش و خونسردی» دعوت می کند، اینبار با صدای بلند هشدار می دهد:

دولت بریتانیا مدعی شد تهدیدات سایبری می توانند بسیار خطرناک تر از یک حمله اتمی باشند (کمیته امور داخلی بریتانیا،۶ آگوست ۲۰۱۳)

فعالیت امنیت سایبری آمریکا

United States Army Cyber Command

فرماندهی سایبری ارتش ایالات متحده

- فعالیت: از سال ۲۰۱۰ تاکنون
- شاخه: نیروی زمینی ایالات متحده آمریکا
- نوع فعالیت: تهدیدات پیشرفته و مستمر عملیات سایبر
- پادگان: فورت گوردن، ایالت جورجیا
- نام مستعار: ARCYBER
- فرمانده کنونی: ژنرال پل م. ناکاسون

فعالیت امنیت سایبری آمریکا

- آژانس امنیت ملی آمریکا که نهاد اطلاعاتی وزارت دفاع به شمار می رود ، فرماندهی تدارک برای مقابله با جنگ سایبری را به عهده گرفته است.
- تصویب لایحه راهبرد هماهنگ کننده برای موضوعات فضای سایبری و امنیت سایبری جهانی
- تاسیس سفارت سایبری آمریکا و انتخاب سفیر در فضای مجازی
- انتخاب سفیر سایبری بعنوان مشاورز اصلی وزیر خارجه
- تاسیس قرارگاه فرماندهی سایبری
- توسعه راهبرد آتش پشتیبان سایبری تهاجمی مانند آتش توپخانه در خط مقدم
- برنامه‌ریزی و تحلیل هدف‌یابی سایبری با اهداف نظامی؛ فرآیند تلفیق آتش‌های مشترک و تأثیرات مرگبار و غیرمرگبار آن
- تجهیز نیرو ویژه با تسلیحات سایبری در کنار تفنگ‌ها، توپخانه، تانک‌ها، بالگردها و هواپیماها در میدان نبرد
- صدور مجوز حملات پیشگیرانه سایبری مقابل کشورهایی نظیر چین، روسیه و ایران
- برنامه ریزی برای توسعه راهبرد مشترک با دولتهای هم پیمان در زمینه دفاع سایبری
- تلقی کردن حملات سایبری بعنوان اقدامات جنگی و حق مقابله به مثل
- بهره گیری از استعدادها و مهارت های کشور از طریق نیروی کاری سایبری استثنایی و نوآوری سریع در فناوری.

فعالیت امنیت سایبری اسرائیل

- **شروع فعالیت**: اطلاعاتی دقیق در دسترس نیست ولی برخی از منابع از دهه ۱۹۳۰ را اعلام می کنند
- **شاخه**: یکی از یگانهای نیروی اطلاعاتی ارتش اسرائیل
- **نوع فعالیت**: جمع‌آوری داده‌های مجازی، جاسوسی از ایمیل‌ها و اطلاعات اینترنتی در کنار رمزگشایی از کدها
- **پادگان**: گیلوت، شمال تلاویو
- **میزان فعالیت**: هیچ عملیات اطلاعاتی در اسرائیل وجود ندارد که یگان ۸۲۰۰ در آن حضور نداشته باشد.
- **جایگاه**: بزرگترین واحد در وزارت دفاع رژیم صهیونیستی از نظر تعداد نیروها است

Unit 8200
یگان ۸۲۰۰

فعالیت امنیت سایبری اسرائیل

- به ادعای رژیم صهیونیستی، سربازان یگان ۸۲۰۰ در علوم رایانه و فناوری اطلاعات در جهان سرآمد هستند.
- تأسیس دفتر ملی سایبری اسرائیل(INCB) برای مبارزه با مشکلات سایبری
- سازمان نظارت بر بانک مرکزی اسرائیل حدود سه سال پیش برای تقویت بخش بانکی و مالی اسرائیل در برابر حملات سایبری ایجاد شد
- اتخاذ رویکرد بهترین حمله، بهترین دفاع است و در حوزه سایبری بسیار مهم است که حمله‌کننده شناخته شود.
- موشه یعلون، نخست‌وزیر این رژیم، ادعا کرده است که اسرائیل می‌تواند در حوزه‌ی سایبر دشمنان خود را خلع سلاح کند و به‌عنوان قدرت سایبری مطرح شود.
- همیشه سعی دارد که خود را قربانی حملات نشان دهد و از حملاتی که خود به دیگر کشورها می‌کند سخن به میان نمی‌آورد
- اجرای مستمر مانورهای سایبری و شبیه سازی جنگ سایبری
- تنظیم قانون ۲۰۱۶ تقویت همکاری در زمینه امنیت سایبری بین امریکا و اسرائیل(H.R. 5843)
- تأسیس مدرسه جنگ سایبری برای مقامات نظامی این رژیم است تا فرماندهان با جنگ سایبری هرچه بیشتر آشنا شوند.
- جذب بیش از ۴۵۰میلیون دلار سرمایه گذاری خارجی در شرکت های امنیت سایبری اسرائیل
- WAZEیکی از افتخارات یگان مخفی ۸۲۰۰ ارتش اسرائیل

نمونه از جنگ های مجازی

- در سال ۲۰۰۶م. در جریان جنگ حزب‌اللّه و اسراییل، دولت صهیونیستی اعلام کرد که مورد حملات سایبری سازمان یافته از طرف کشورهای خاورمیانه و روسیه قرار گرفته است.
- در سال ۲۰۰۷م. این بار کشور «استونی» بود که خبر از حمله‌ی سایبری به خود داد. هدف این حمله گویا رسانه‌ها، بانک‌ها و وزارتخانه‌های این کشور بودند که از سوی سروری در روسیه مورد حمله قرار گرفتند.
- در سال ۲۰۰۷م.، تارنمای انتخابات کشور «قزاقستان» در جریان یک حمله‌ی سایبری از کار افتاد.
- در سال ۲۰۰۸م.، سایت‌های مربوط به کشورهای روسیه، گرجستان و آذربایجان در جریان درگیری‌ها در اوستیای جنوبی مورد حمله‌ی هکرها قرار گرفتند.
- در سال ۲۰۰۹م.، حملات گسترده‌ای به بخش‌های دولتی، رسانه‌ای و تارنماهای مالی ایالات متحده و کره جنوبی صورت پذیرفت. در حالی که همه به راه‌اندازی حمله از سوی کره شمالی نظر داشتند یک تحقیق نشان داد که با کمال تعجب حمله از یک سرور ناشناخته در بریتانیا بوده است.

جنگ و نبرد اطلاعاتی

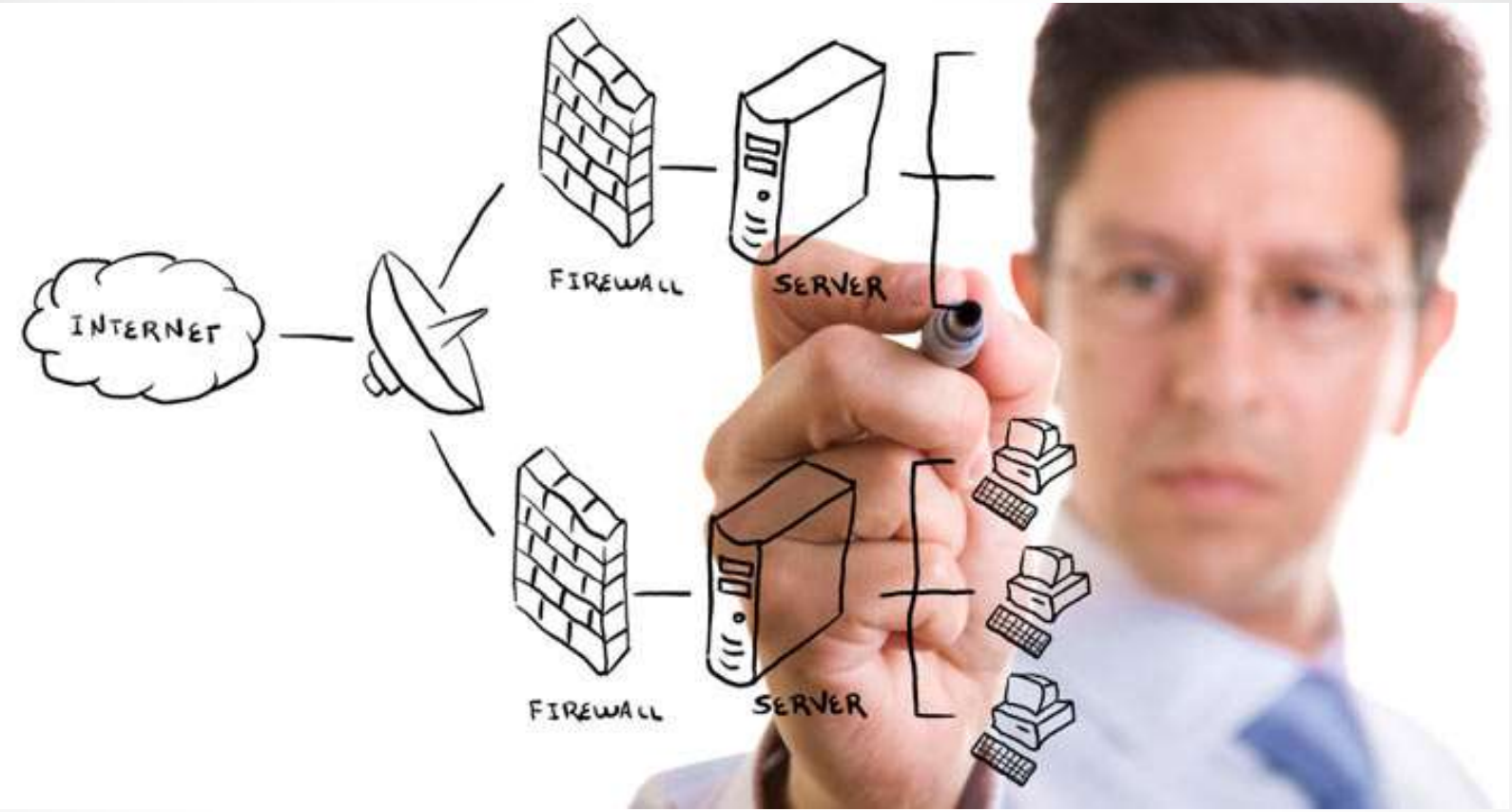
نبرد تدافعی(Defensive)

شامل کلیه استراتژی ها و فعالیـت هـای دفـاعی در برابر حملات بر روی دارایی های ITC می باشد.

نبرد تهاجمی (Offensive)

شامل حمله به دارایی های ITC دشمن می باشد.


جنگی که بود
راهی که هست
www.irna.ir
Iran News Agency



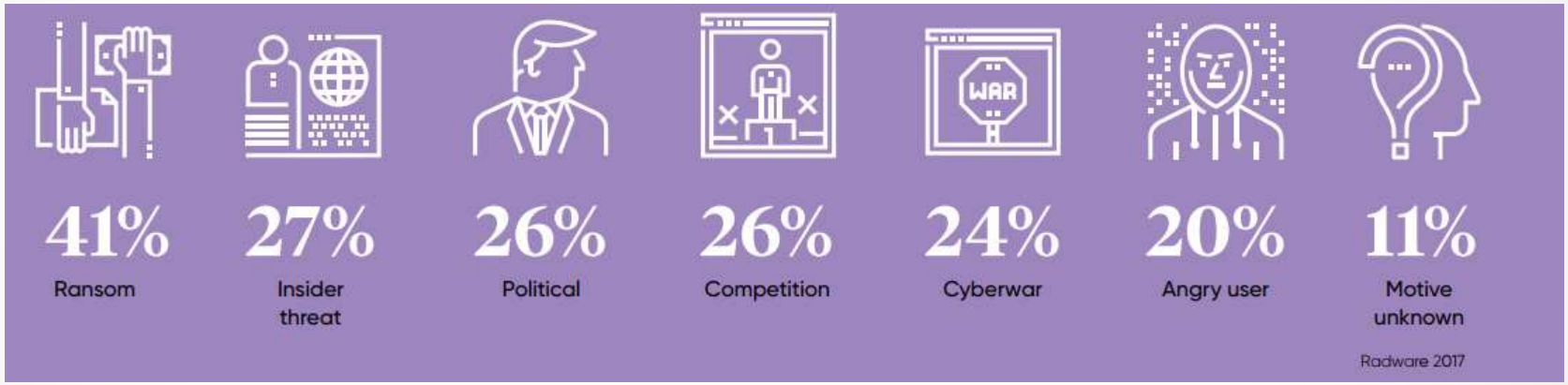
مفاهیم امنیت اطلاعات

حمله چیست؟

Motive(Goal) + Method + Vulnerability

نقطه آسیب پذیــری + روش + انگیــزه ذهنــی(هدف)

انگیزه حمله


41%
Ransom
27%
Insider threat
26%
Political
26%
Competition
24%
Cyberwar
20%
Angry user
11%
Motive unknown
Radware 2017

تعاریف و مفاهیم اولیه

- **آسیب‌پذیری (Vulnerability):** ویژگی یا نقطه ضعفی در سیستم که می توان از آن سوءاستفاده کرد و امنیت سیستم را نقض کرد.
- **حمله (Attack):** تلاش برای یک نفوذ عمدی در یک سیستم اطلاعاتی/ ارتباطی، حمله گفته می‌شود (معمولاً با بهره‌گیری از آسیب‌پذیری‌های موجود).
- **نفوذ (Intrusion):** نتیجه یک حمله موفق و نقض امنیت سیستم.
- **مکانیزم امنیتی (Security Mechanism):** به هر روش، ابزار و یا رویه‌ای که برای اعمال یک سیاست امنیتی به کار می‌رود، یک مکانیزم امنیتی گویند.
- **خطمشی (سیاست) امنیتی(Security Policy):** نیازمندیهای امنیتی یک سازمان و یا یک سیستم اطلاعاتی/ ارتباطی را بیان می‌نماید.

تعاریف و مفاهیم اولیه

- **محرمانگی (confidentiality):** جلوگیری از افشای اطلاعات به افراد غیرمجاز
- **جامعیت (integrity:** جلوگیری از تغییر داده‌ها به‌طور غیرمجاز و تشخیص تغییر در صورت دستکاری غیرمجاز اطلاعات
- **دسترس پذیری (availability):** اطلاعات باید زمانی که مورد نیاز توسط افراد مجاز هستند در دسترس باشند.

انواع حملات

شنود یا Interception
در این روش نفوذگر به شکل مخفیانه از اطلاعات نسخه برداری می کند.

تغییر اطلاعات یا Modification
در این روش نفوذگر به دستکاری و تغییر اطلاعات می‌پردازد.

افزودن اطلاعات یا Fabrication
در این روش نفوذگر اطلاعات اضافی بر اصل اطلاعات اضافه می‌کند.

وقفه Interruption
در این روش نفوذگر باعث اختلال در شبکه و تبادل اطلاعات می‌شود.

هکر کیست؟

Who Is Hacker?

Excellent Computer Skills
مهارت های عالی کامپیوتر

unauthorized access to data
دسترسی غیرمجاز به داده

Do Illegal Things
انجام کارهای غیرقانونی

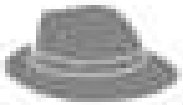
انواع هکر

White hat hackers

هکرهای کلاه سفیدیا هکر خوب، متخصصین شبکه هستند که
چاله‌های امنیتی شبکه را پیدا می کنند

Black hat hackers

هکرهای کلاه سیاه اشخاصی هستند که با وارد شدن به شبکه و
دستبرد اطلاعات یا جاسوسی کردن، سوءاستفاده می کنند



Gray hat hackers

هکرهای کلاه خاکستری حد وسط دو تعریف بالا می باشند

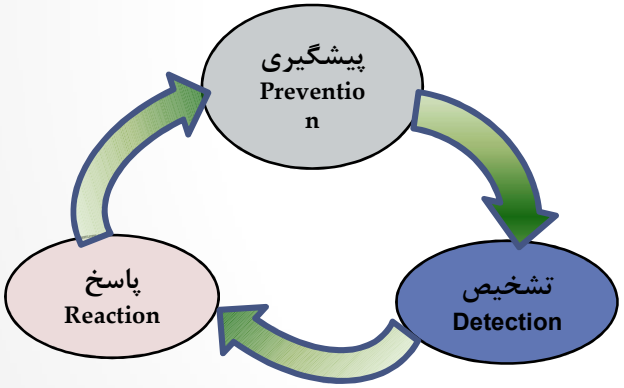
Pink hat hackers

هکرهای کلاه صورتی افراد کم سوادی هستند که با چند نرم‌افزار
خرابکارانه به آزار و اذیت دیگران می پردازند

منشا تهدیدات

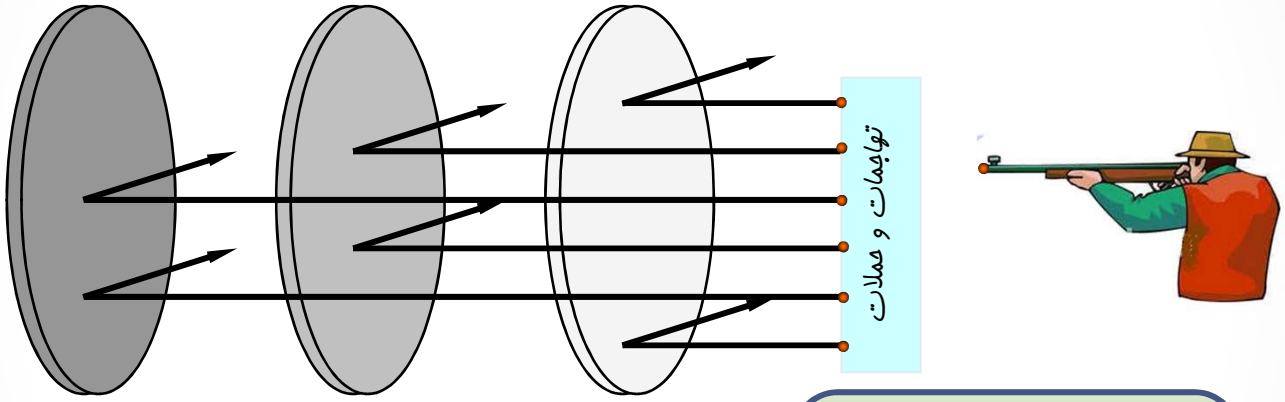
اقدامات امنیتی

- **پیشگیری (Prevention)**
  - جلوگیری از خسارت
- **تشخیص و ردیابی (Detection & Tracing)**
  - تشخیص (Detection)
    - میزان خسارت
    - هویت دشمن
    - کیفیت حمله (زمان، مکان، دلایل حمله، نقاط ضعف...)
- **پاسخ (Reaction)**
  - ترمیم، بازیابی و جبران خسارات
  - جلوگیری از حملات مجدد



اقدامات امنیتی

- مراتب مقابله با نفوذ و تهاجم در سیستم اطلاعاتی / ارتباطی



- شناسایی و احراز هویت
- کنترل دسترسی
- حفاظ (دیواره آتش)
- رمزنگاری و امضای دیجیتال

تکرار د

- سیستم تشخیص نفوذ (IDS)
- سیستم همبسته‌ساز رویدادها
- سیستم تله‌عسل (Honeypot)

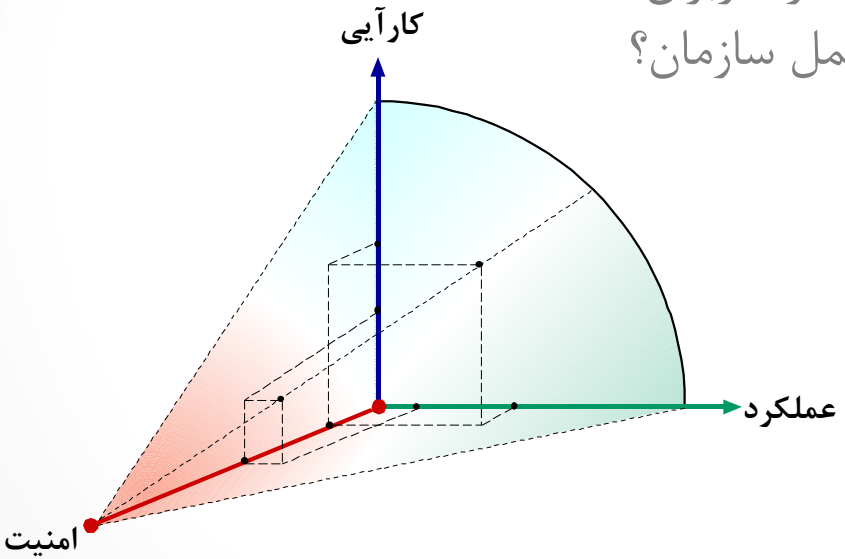
دلایل نا امنی سیستم ها

- **ضعف فناوري**
  - پروتكل، سيستم عامل، تجهيزات
- **ضعف تنظيمات**
  - رهاكردن تنظيمات پيش‌فرض، گذرواژه‌هاي نامناسب، عدم استفاده از رمزنگاري، راه‌اندازي سرويس‌هاي اينترنت بدون اعمال تنظيمات لازم، ...
- **ضعف سياست‌گذاري**
  - عدم وجود سياست امنيتي
  - عدم وجود طرحي براي مقابله با تهديدات و مخاطرات
  - نداشتن نظارت امنيتي مناسب (مديريتي و فني)

ضعف مدیریتی

استراتژی امنیت سازمانی

- مصالحه بین امنیت، کارآیی و عملکرد
- مصالحه بین امنیت، کارایی و هزینه
- میزان امنیت مورد انتظار کاربران؟
- میزان ناامنی قابل تحمل سازمان؟



دشواری برقراری امنیت

- افزایش پیچیدگی و تهدید امنیت بدلیل تکامل پروتکلها
- امنیت: قربانی افزایش کارایی و مقیاس پذیری
- امنیت بالا: هزینه بر
- در اختیار بودن اطلاعات و ابزارهای دور زدن امنیت
- مبارزه و لذت بردن از دور زدن امنیت
- عدم در نظر گرفتن ملاحظات امنیتی در طراحی های اولیه سیستمها و شبکه ها
- امنیت معمولاً قربانی افزایش کارآیی و مقیاس پذیری می‌شود.
- بعنوان مانع در برابر انجام کار کاربران عادی عدم پیروی از سیاستهای امنیتی

تهدیدات امنیت اطلاعات