
بسم الله الرحمن الرحيم

امنیت سایبری

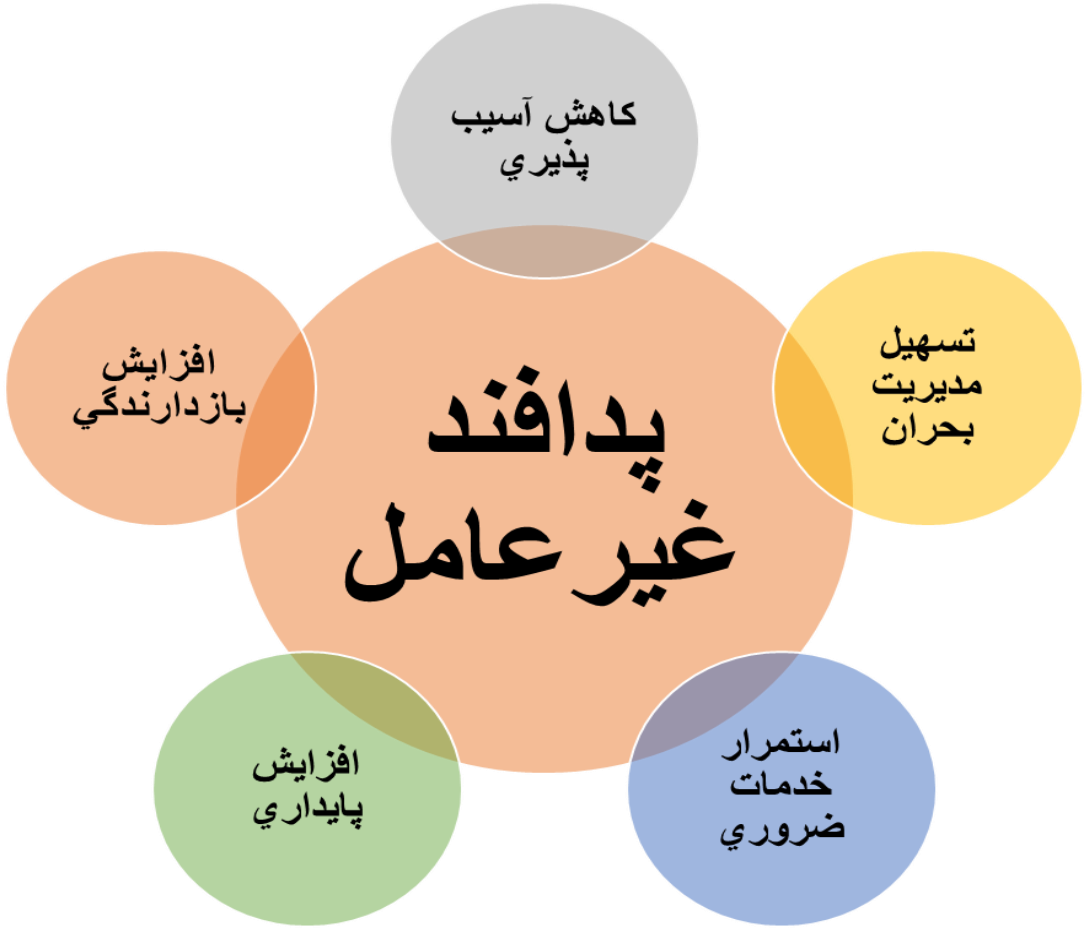
مهندس محسن رمضانی

تیرماه ۱۴۰۴

تعریف پدافند غیر عامل «مطابق مصوبه مجمع تشخیص مصلحت نظام و ابلاغ مقام معظم رهبری از سال ۱۳۸۹»

**عبارت است از مجموعه اقدامات غیر مسلحانه که موجب افزایش بازدارندگی،
کاهش آسیب‌پذیری،
تداوم فعالیت‌های ضروری،
ارتقاء پایداری ملی
و تسهیل مدیریت بحران
در مقابل تهدیدات و اقدامات نظامی دشمن می‌گردد.**

کلیدواژه های پدافند غیرعامل



بازدارندگی

بازدارندگی: اتخاذ تدابیر گوناگون از سوی یک دولت یا گروهی از دولت‌ها برای **مأیوس** کردن دولت یا دولت‌های دیگر از پیگیری سیاست‌های تهدیدآمیز

مهم‌ترین عامل بازدارندگی

قدرت ملی: مجموعه توانایی‌های مادی و معنوی در قلمرو یک واحد جغرافیایی و سیاسی به نام کشور یا دولت که معمولا متشکل از برآیند همه مؤلفه‌های قدرت است.

کاهش آسیب پذیری

کاهش آسیب‌پذیری

مفهوم مقابل آسیب‌پذیری = مصونیت

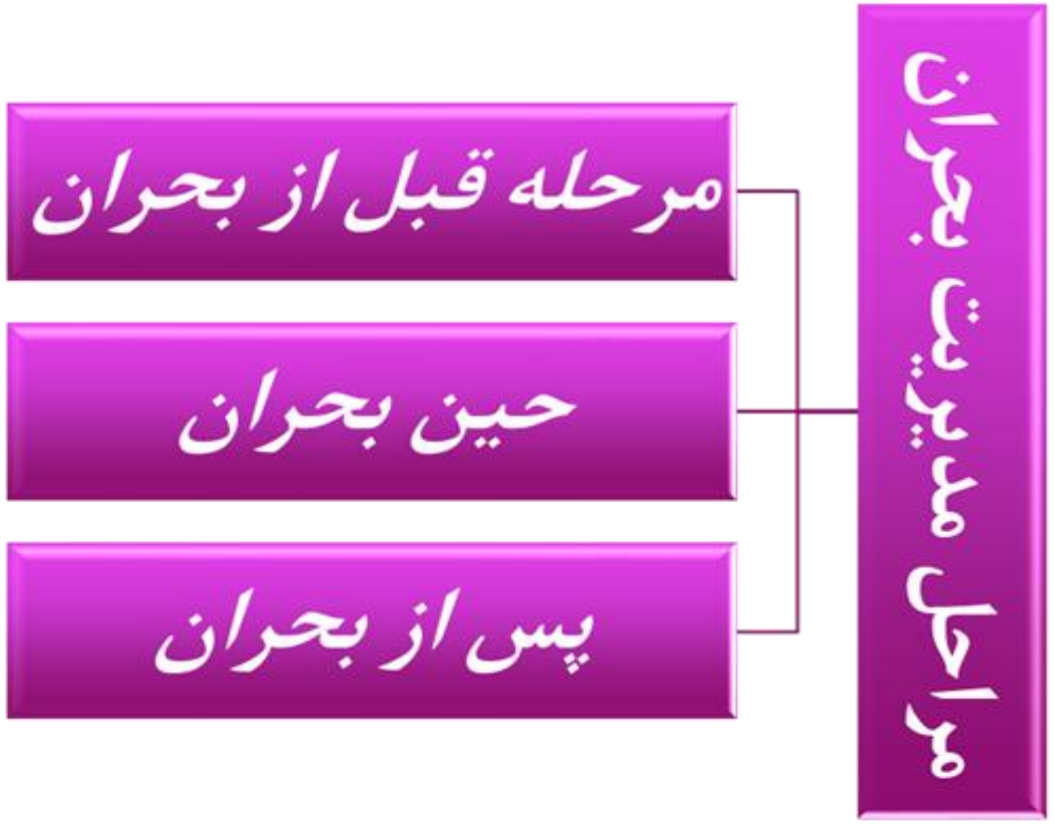
مصونیت‌سازی در برابر تهدیدات = کاهش تأثیر تهدیدات به جامعه و پیکره کشور در اثر مقاوم‌سازی آن.

مقام معظم رهبری: مصونیت یعنی اینکه ولو دشمن تهاجمی بکند و زحمتی هم بکشد و ضرب و زوری هم بزند، اثری نخواهد کرد.

تداوم فعالیت های ضروری

تأمین حداقلِ شرایط فعالیت برای رفع نیازهای جامعه و اداره تمامی امور در شرایط بحران

تسهیل مدیریت بحران



ارتقاء پایداری ملی

ایستادگی، ثبات قدم و مقاومت ملی در برابر ناملایماتی که از سوی دول بیگانه و متخاصم بر مردم و کشور تحمیل گردیده و موجب حفظ تعادل ملی و ارتقاء ضریب امنیت ملی کشور در مقیاس ملی، استانی و محلی می‌گردد

مفهوم فضای سایبری

فضای سایبری به معنی شبکه های وابسته به یکدیگر از زیرساخت فناوری اطلاعات که حداقل از ۴ قسمت زیر تشکیل شده است:

- اینترنت
- شبکه های مخابراتی
- پردازشگرها
- سیستم های کامپیوتری

اصطلاحات امنیت سایبری

حمله

attack

آسیب پذیری

Vulnerability

مکانیزم امنیتی

Security Mechanism

سیاست امنیتی

Security policy

نفوذ

Intrusion

اصطلاحات امنیت سایبری

CAPTCHA

BUG

SSL

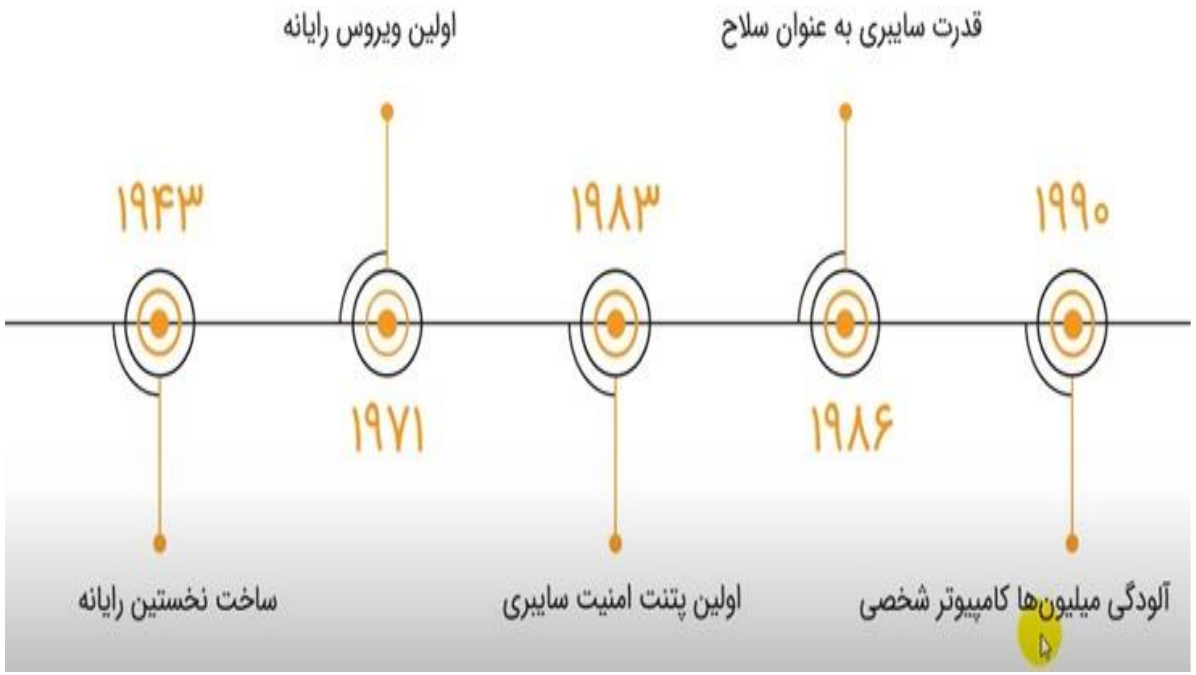
FIREWALL

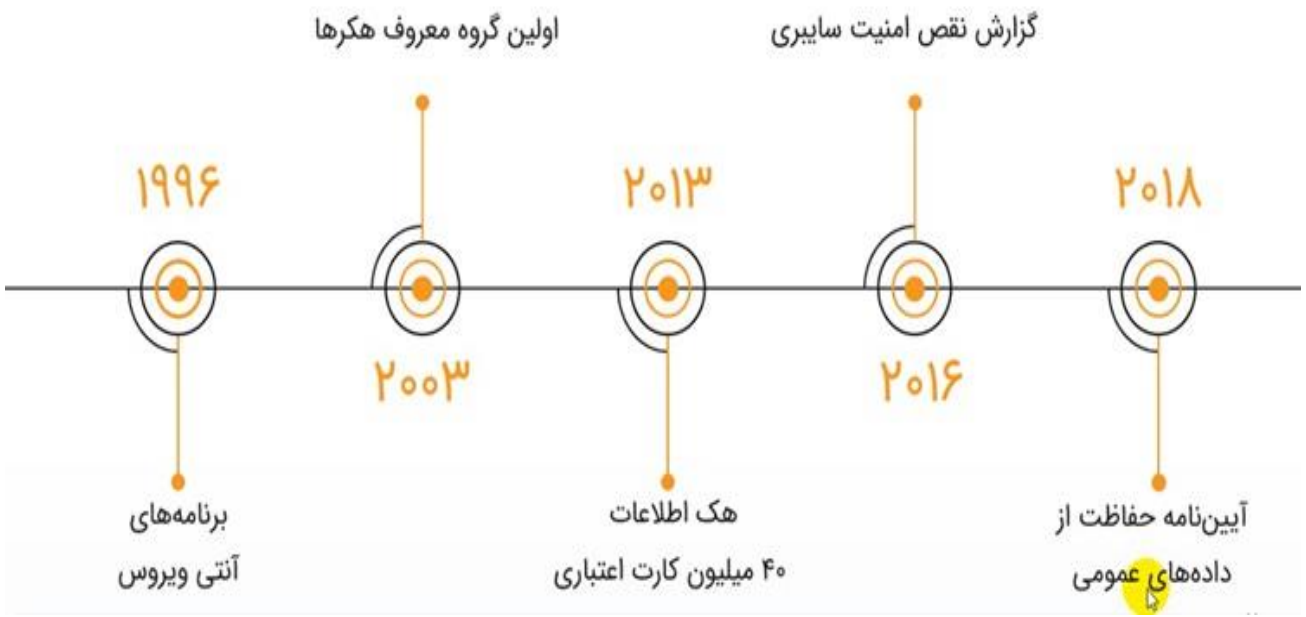
COOKIE

خصوصیات فضای سایبری

- انتزاعی بودن
- ناملموس بودن
- قلمرو بی نهایت
- غیرقابل کنترل بودن
- دسترسی آسان
- تخصصی بودن فضا
- وسعت ضرر

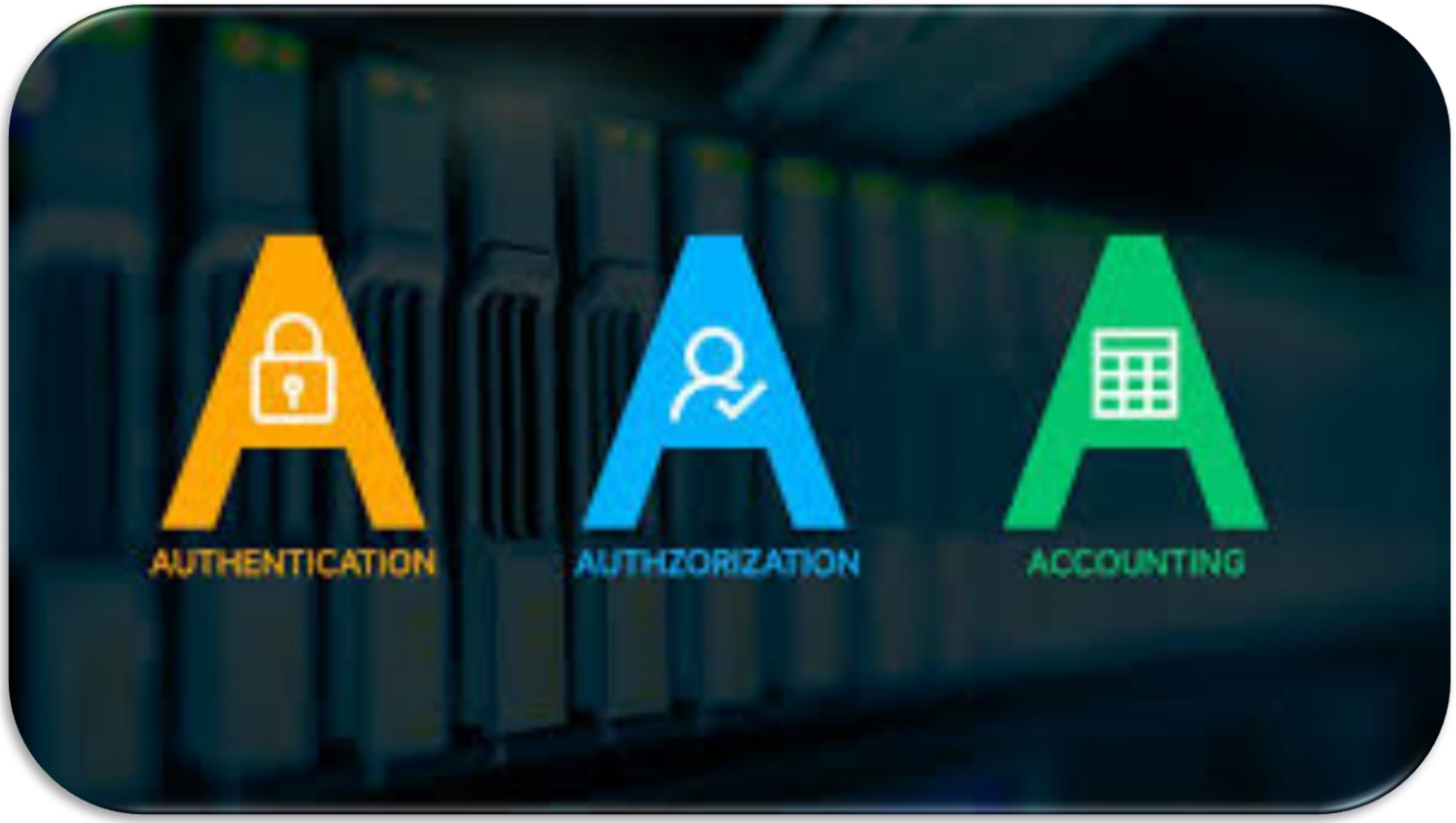
تاریخچه امنیت سایبری





اهداف یا اصول بنیادین امنیت اطلاعات

مکانیزم هایی برای رسیدن به اهداف امنیت



انواع هکرها

کلاه خاکستر

کلاه سیاه

کلاه سفید

ری

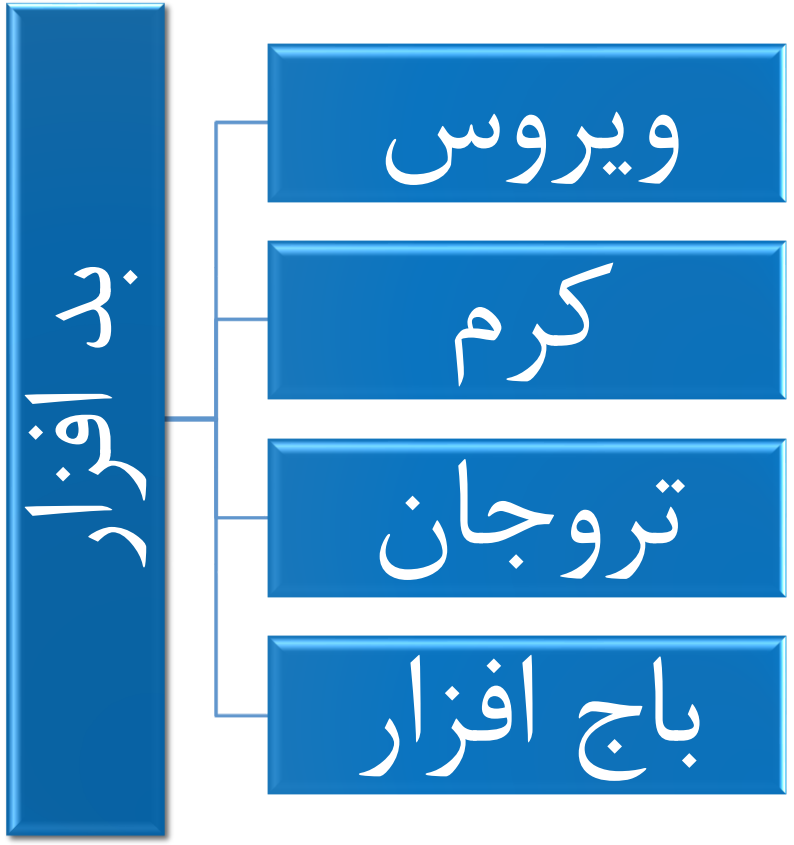
تهدیدات سایبری Cyber Threats

تهدیدات سایبری به هرگونه اقدام، رخداد یا شرایطی گفته می‌شود که **امنیت سیستم‌های اطلاعاتی، داده‌ها یا شبکه‌ها را به خطر می‌اندازد**. این تهدیدات می‌توانند باعث از بین رفتن محرمانگی، یکپارچگی یا دسترس‌پذیری اطلاعات شوند.

دسته‌بندی تهدیدات سایبری

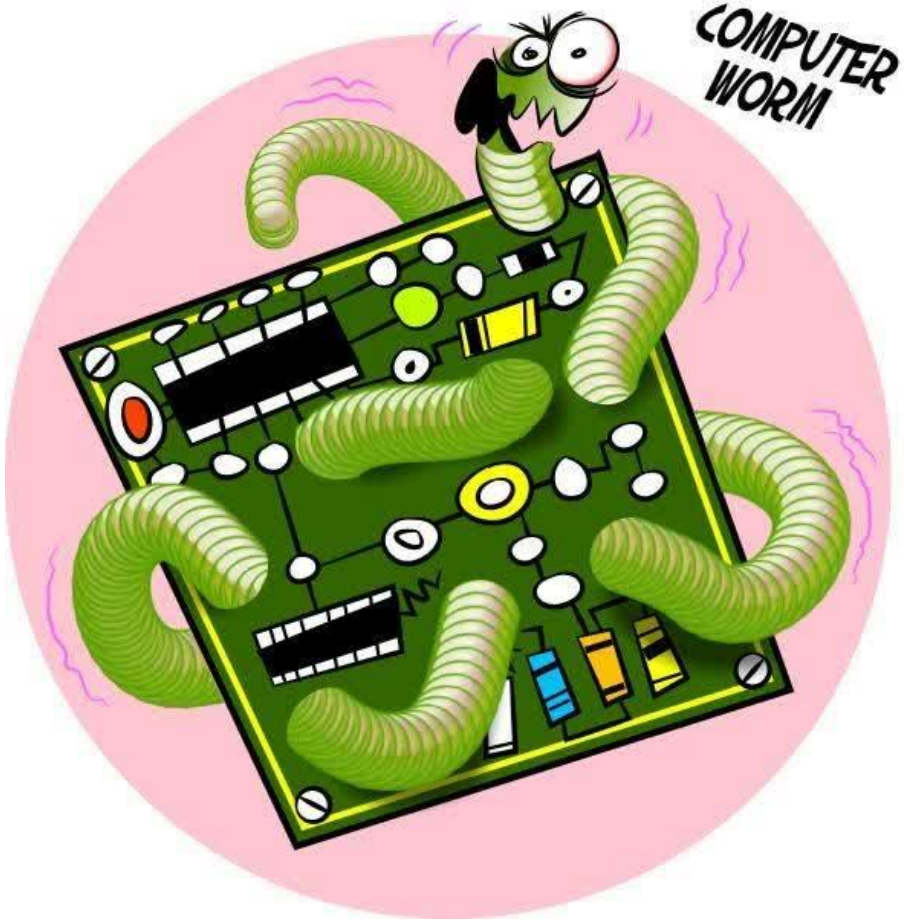
بر اساس منبع تهدید	• داخلی • خارجی
بر اساس نوع حمله	• فعال • غیرفعال
بر اساس هدف تهدید	• داده • نرم افزار شبکه کاربران
بر اساس روش اجرا	• بدافزار • آسیب‌پذیری‌ها مهندسی اجتماعی حملات شبکه‌ای

تهدید بر اساس روش اجرا



Virus

Worm



Trojan

Ransomware

مهندسی اجتماعی

(سوءاستفاده از خطاها، اعتماد یا ناآگاهی انسان برای دسترسی به اطلاعات یا سیستم)

مثال	توضیح	روش
ایمیل جعلی از بانک برای دریافت رمز کارت	ارسال ایمیل/پیام جعلی برای گرفتن اطلاعات	فیشینگ ((Phishing)
تماس از "پشتیبانی مایکروسافت" برای نصب نرم‌افزار مخرب	تماس صوتی جعلی برای فریب فرد	ویشینگ ((Vishing)
پیامک با لینک جایزه یا قطع یارانه	فیشینگ از طریق پیامک	اسمیشینگ ((Smishing)
"من از ITهستم، رمزت رو بده تا مشکل رو حل کنم"	ساختن یک سناریوی جعلی برای اعتمادسازی	زمینه‌سازی((Pretexting
فلش مموری رها شده در راهرو شرکت	ارائه فایل یا وسیله وسوسه‌انگیز (مثل فلش مموری آلوده)	طعمه‌گذاری((Baiting

سوء استفاده از آسیب پذیری ها

هکرها از باگ‌ها یا حفره‌های امنیتی در نرم‌افزار، سیستم عامل یا سرویس‌ها استفاده می‌کنند تا کنترل سیستم را به‌دست بگیرند.

روش	توضیح	مثال
SQL Injection	وارد کردن دستورات SQLمخرب در فرم‌ها یا URLها	دسترسی به پایگاه داده سایت فروشگاهی
Cross-Site Scripting (XSS)	وارد کردن کد جاوااسکریپت در صفحات سایت	دزدیدن کوکی کاربران سایت
Buffer Overflow	نوشتن بیش از حد در حافظه موقت و اجرای کد مخرب	استفاده برای اجرای Shellمخفی
Zero-Day Attack	حمله به باگ‌هایی که هنوز توسط توسعه‌دهنده اصلاح نشده‌اند	حمله به Adobe Flashپیش از ارائه وصله امنیتی

حملات شبکه‌ای (Network Attacks)

هدف این نوع حملات دستکاری، شنود یا قطع ارتباط در سطح شبکه است.

نوع	توضیح	مثال
Man-in-the-Middle (MITM)	نفوذگر بین دو ارتباط قرار می‌گیرد و اطلاعات را می‌بیند یا تغییر می‌دهد	شنود HTTPS در وای‌فای عمومی
ARP Spoofing	جعل آدرس MAC در شبکه محلی برای شنود یا هدایت ترافیک	مشاهده ترافیک سایر کاربران شبکه
DNS Spoofing	جعل پاسخ DNS برای هدایت کاربران به سایت جعلی	ورود به سایت بانک، اما رفتن به سایت هکر
Packet Sniffing	ضبط و تحلیل بسته‌های شبکه برای استخراج اطلاعات	Wireshark برای گرفتن رمز عبور ساده
DDoS Attack	فرستادن حجم بالای درخواست به سرور برای از کار انداختن آن	حمله به Amazon AWS در ۲۰۲۰

جمع بندی تفاوت ها

نیاز به تعامل انسانی	پیچیدگی فنی	تمرکز اصلی	دسته
نه	بالا	تخریب یا سرقت اطلاعات از درون سیستم	بدافزارها
بله ✅	پایین تا متوسط	فریب انسان‌ها برای افشای اطلاعات	مهندسی اجتماعی
خیر	بسیار بالا	بهره‌برداری از باگ‌های نرم‌افزاری	سوءاستفاده از آسیب‌پذیری
گاهی	متوسط تا بالا	اختلال یا شنود در مسیر ارتباطی	حملات شبکه‌ای

پیشگیری از تهدیدات سایبری

باج‌افزار (Ransomware)

- **راه‌های پیشگیری:**

- تهیه نسخه پشتیبان منظم از فایل‌ها (روی سیستم جداگانه)
- عدم کلیک روی پیوست‌ها و لینک‌های ایمیل‌های مشکوک
- به‌روزرسانی سیستم‌عامل و نرم‌افزارها

- **مثال:**

حمله WannaCry در سال ۲۰۱۷ سیستم‌های بیمارستانی و شرکت‌ها را آلوده کرد و باعث قفل شدن اطلاعات شد.

ادامه

فیشینگ(Phishing)

- **راه‌های پیشگیری:**

- آموزش کاربران برای شناسایی ایمیل‌های فیشینگ
- استفاده از فیلتر ایمیل‌ها و ابزارهای ضدفیشینگ
- بررسی لینک‌ها و آدرس فرستنده پیش از کلیک

- **مثال:**

ایمیلی جعلی به کارمند ارسال می‌شود که حاوی لینک ورود است؛ پس از وارد کردن رمز، حساب وی هک می‌شود.

ادامه

مهندسی اجتماعی(Social Engineering)

- **راه‌های پیشگیری:**

- آموزش کارکنان برای شناسایی روش‌های فریب
- عدم افشای اطلاعات به افراد مشکوک حتی با ظاهر رسمی

- **مثال:**

هکری با تماس تلفنی، خود را از بخش IT معرفی می‌کند و از کارمند رمز عبور می‌گیرد.

ادامه

ویروس و کرم(Virus & Worm)

- **راه‌های پیشگیری:**

- نصب و بروز نگه داشتن آنتی‌ویروس
- عدم اتصال فلش مموری‌های ناشناس
- محدود کردن اجرای فایل‌های مشکوک

- **مثال:**

فلش آلوده‌ای به سیستم متصل شده و کرمی از طریق شبکه پخش می‌شود.

ادامه

حملاتDDoS

- **راه‌های پیشگیری:**

- استفاده از فایروال و سیستم مقابله باDDoS
- تقسیم بار روی چند سرور(Load Balancing)
- همکاری با ISP برای فیلتر درخواست‌های مخرب

- **مثال:**

وب‌سایت بانک در زمان پرتقاضا از دسترس خارج می‌شود به‌دلیل دریافت حجم زیادی درخواست جعلی.

ادامه

تهدیدات داخلی(Insider Threat)

🔹 **راه‌های پیشگیری:**

- استفاده از اصل حداقل دسترسی(Least Privilege)
- ثبت لاگ فعالیت کاربران
- استفاده از سیستم‌های DLP برای جلوگیری از خروج اطلاعات

🔸 **مثال:**

کارمندی پیش از خروج از شرکت، لیست مشتریان را به ایمیل شخصی خود ارسال می‌کند.

ادامه

حملات SQL Injection

- **راه‌های پیشگیری:**
  - استفاده از کوئری‌های امن
  - اعتبارسنجی ورودی کاربران
  - بروزرسانی CMS و پایگاه داده
- **مثال:**

هکر با وارد کردن عبارت مخرب در فرم جستجو، اطلاعات پایگاه داده را حذف می‌کند.

ادامه

سرقت اطلاعات حساب کاربری

🔹 **راه‌های پیشگیری:**

- استفاده از احراز هویت چندمرحله‌ای(MFA)
- تغییر رمزهای پیش‌فرض و استفاده از رمز قوی
- عدم ذخیره رمز عبور به صورت ناامن

🔸 **مثال:**

کاربر رمز را روی میز یادداشت کرده و فردی آن را دیده و سوءاستفاده می‌کند.

سوءاستفاده از هوش مصنوعی در حملات سایبری

تحلیل تهدیدات نوین مبتنی بر AI

جعل چهره و صدا
(Deepfake for Social Engineering)

- استفاده از هوش مصنوعی برای شبیه‌سازی صدای افراد جهت فریب قربانیان.

✅مثال واقعی :در سال 2019، صدای مدیریک شرکت شبیه‌سازی شد و مدیرعامل شرکت قربانی 243,000دلار به حساب هکر واریز کرد.

فیشینگ هوشمند (AI-Powered Phishing)

- AI 🔹 می‌تواند ایمیل‌های بسیار واقعی، بدون خطا و شخصی‌سازی‌شده تولید کند.

✅مثال :ایمیلی ظاهراً از سوی رئیس شما، با محتوای مرتبط با پروژه‌های واقعی، شامل لینک آلوده.

بدافزار تطبیق‌پذیر با AI (Adaptive Malware)

- بدافزارهایی که با استفاده از یادگیری ماشین از شناسایی فرار می‌کنند.

✅مثال :بدافزاری که در محیط آزمایشگاهی غیرفعال می‌ماند اما در سیستم واقعی فعال می‌شود.

تحلیل دفاع‌ها با AI (AI-based Reconnaissance)

- AI 🔹 شبکه را تحلیل می‌کند تا زمان و مکان مناسب حمله را شناسایی کند.

✅مثال :رباتی که فعالیت‌های فایروال را بررسی می‌کند و در زمان ضعف، حمله را آغاز می‌کند.

نمونه‌های واقعی حملات سایبری و مهندسی اجتماعی

Stuxnet (2009–2010)

🔹 نوع حمله :بدافزار صنعتی

📌 توضیح :اولین ویروس صنعتی دنیا برای خرابکاری در تأسیسات هسته‌ای ایران .توسط آمریکا و اسرائیل طراحی شد.

Sony Pictures Hack (2014)

🔷 نوع حمله :نشت اطلاعات و تخریب

📌 توضیح :حمله گروه Lazarusبه دلیل انتشار فیلمی ضد کره شمالی .

اطلاعات کارکنان و فیلم‌ها افشا شد.

Yahoo Breach (2013–2014)

🔹 نوع حمله :نشت داده

📌 توضیح :اطلاعات ۳میلیارد حساب کاربری فاش شد .بزرگ‌ترین نشت داده تاریخ تا آن زمان.

WannaCry (2017)

- نوع حمله :باج‌افزار جهانی

📌 توضیح :قفل کردن فایل‌ها در بیمارستان‌ها و شرکت‌ها با درخواست باج .از آسیب‌پذیری SMBاستفاده شد.

Equifax Breach (2017)

- نوع حمله :آسیب‌پذیری نرم‌افزاری

📌 توضیح :اطلاعات بیش از ۱۴۰میلیون آمریکایی از جمله SSN و اطلاعات هویتی فاش شد.

Twitter Bitcoin Scam (2020)

🔷 نوع حمله :مهندسی اجتماعی

📌 توضیح :نفوذ به پنل توییتر از طریق فریب کارکنان و ارسال پیام‌های کلاهبرداری از حساب افراد مشهور.

Google & Facebook Scam (2013–2015)

🔹 نوع حمله :جعل ایمیل مالی

📌 توضیح :هکر با فاکتور جعلی بیش از ۱۰۰میلیون دلار از گوگل و فیسبوک گرفت.

Target Breach (2013)

🔹 نوع حمله :زنجیره تأمین

📌 توضیح :نفوذ از طریق پیمانکار تهویه و سرقت اطلاعات میلیون‌ها کارت اعتباری.

CEO Fraud – Pathé (2018)

🔷 نوع حمله Pretexting :جعل ایمیل مدیر عامل

📌 توضیح : ۱۹میلیون یورو از حساب شرکت با ایمیل جعلی مدیرعامل خارج شد.

اینترنت اشیا(IoT)

اینترنت اشیا (IoT) یعنی دستگاه‌ها و اشیاء روزمره (مانند یخچال، خودرو، چراغ برق، ساعت، لباس، سنسورها و...) بتوانند از طریق اینترنت داده ارسال و دریافت کنند.

اجزای اصلی اینترنت اشیا

- سنسورها و تجهیزات جمع‌آوری داده (مثلاً دماسنج، شتاب‌سنج، دوربین)
- اتصال به شبکهWi-Fi ، بلوتوث،4G/5G ،
- پردازشگر و واحد کنترل مثلاً میکروکنترلر یا مینی‌کامپیوتر
- -فضای ابری (Cloud) برای ذخیره و پردازش داده‌ها
- -اپلیکیشن یا داشبورد برای نمایش و تحلیل داده‌ها

مثال‌های کاربردی

مثال از کاربرد اینترنت اشیا	حوزه
کنترل چراغ‌ها یا دما با موبایل	خانه هوشمند
دستگاه کنترل قند خون یا فشار خون متصل به اینترنت	سلامت
ردیابی موقعیت خودروها یا مدیریت ترافیک شهری	حمل و نقل
سنجش رطوبت خاک و آبیاری خودکار	کشاورزی
پایش لحظه‌ای دستگاه‌ها و ماشین‌آلات	صنعت

اهداف اینترنت اشیا

-افزایش کارایی و دقت

-کاهش هزینه‌های عملیاتی

-تصمیم‌گیری هوشمندتر با داده‌های واقعی و لحظه‌ای

-اتومات‌سازی فرآیندها

چالش‌ها و نگرانی‌ها

- امنیت و حریم خصوصی(دستگاه‌ها ممکن است قابل هک شدن باشند)

- استانداردسازی (هماهنگی بین برندها و پروتکل‌ها)

- نیاز به اینترنت پایدار و پرسرعت

سپاس از توجه شما