CYBER DEFENSE

❖ حسین ملک زاده

مشاور و تحلیل گر ارشد امنیت سایبری

کارشناس ارشد امنیت اطلاعات ازدانشگاه Sapienza Universityرم – ایتالیا

مدرس و عضو هیات علمی دانشگاه بین المللی نورث وست Northwest International University

مدرس و عضو هیات علمی دانشگاه نیوجرسی New Jersey International Open University

مدرس و عضو هیات علمی موسسه دانشگاهی DEI Institute - Online Universityآفریقا

دارای مدرک دکترا مدیریت امنیت سایبری DBA - Cyber Security Management از دانشگاه بین المللی نورث وست

ممیز و سرممیز امنیت اطلاعات ISMS ISO27001-2013

دارای مدارک سطح عالی امنیت اطلاعات CISSP , CISA

دارای مدرک مشاور ارشد امنیت سیستمی SSCP

طراح – مشاور و مجری پروژه¬های شبکه و امنیت اطلاعات ISMS , SOC , NOC

دارای بیش از ۲۴ سال سابقه آموزشی – اجرایی و مدیریتی درزمینه پروژه¬های شبکه و امنیت در داخل و خارج از کشور

مدرس دوره¬های تخصصی شبکه و امنیت با بیش از دوازده هزارساعت تدریس درموسسات داخلی و بین المللی

دارای تحصیلات و مدارک بین المللی :

MCSE , CCNA ,CCNA Security , CCNP , CEH , CISSP , CWNA , ISMS , SSCP, GSNA

عضوانجمن مهندسین کامپیوتر و فناوری آمریکا IEEE , ACM

مولف کتاب هنر هک کردن انسان در حوزه امنیت در مهندسی اجتماعی Social engineering

www.Hosseinmalekzadeh.com

Mobile: 09153133217

E-mail: Hoseeinmalekzadeh@Gmail.com

Telegram Channel : https://t.me/HosseinMalekzadeh

http://www.linkedin.com/in/hosseinmalekzadeh

@HOSSEINMALEKZADEH2015

@HOSSEINMALEKZADEH

By. Hossein Malekzadeh

Cyber Security Consultant and Manager

www.Hosseinmalekzadeh.com

Mobile : 09153133217

نقشه شبکه سازمان (دفتر مرکزی)

سناریوی سازمان

یک سازمان متوسط با حدود ۵۰۰ کارمند
دارای دفتر مرکزی و دو شعبه
خدمات اصلی سازمان شامل:

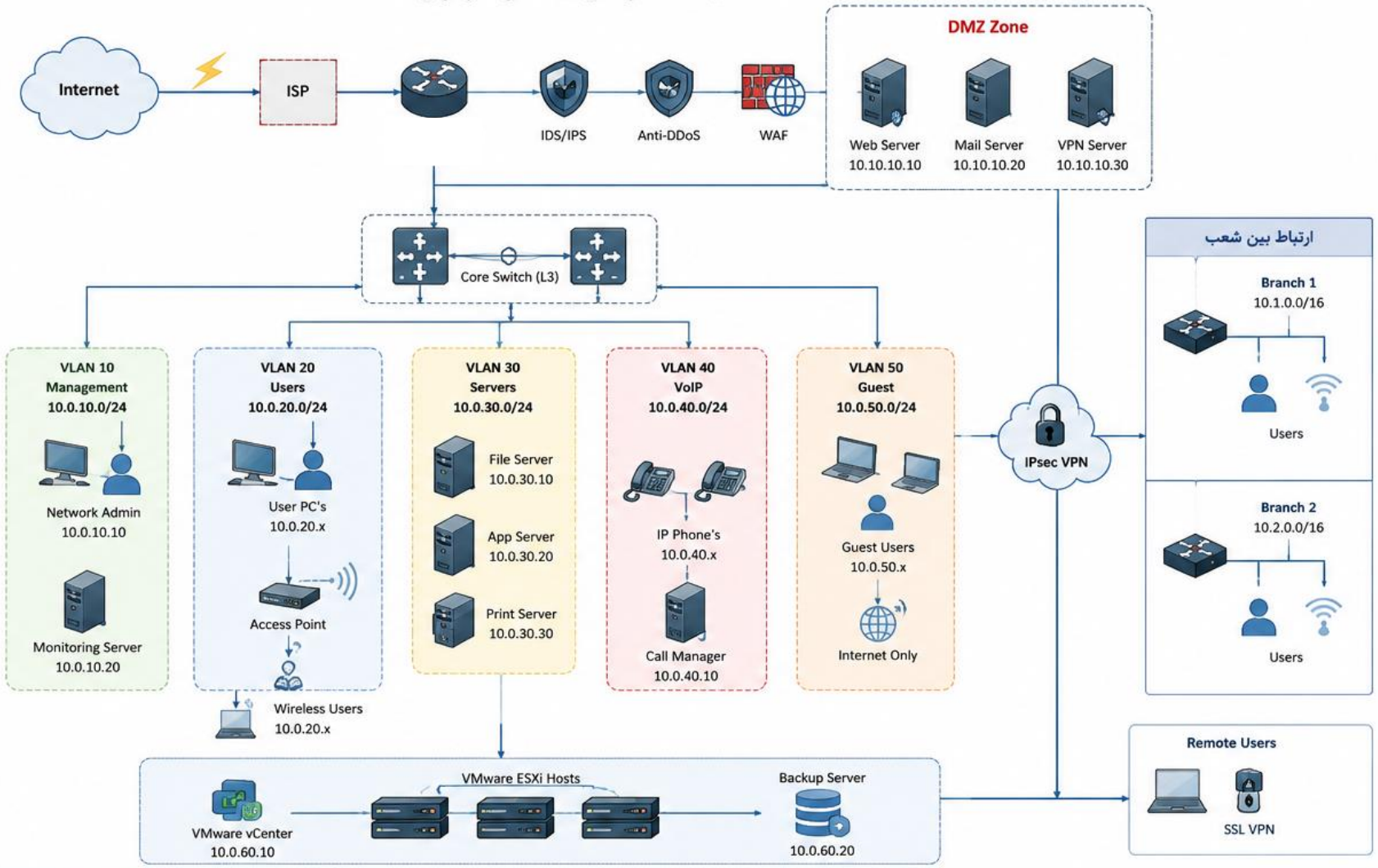
- سرویس های دایرکتوری (Active Directory)
- سرورهای فایل و پرینت
- سرور برنامه کاربردی تحت وب
- سیستم تلفنی تحت شبکه (VoIP)
- دسترسی کاربران به اینترنت
- ارتباط امن بین شعب از طریق VPN
- زیرساخت مجازی سازی با VMware

اهداف امنیتی

- حفاظت لایه به لایه از اطلاعات و سرویس ها
- جلوگیری از دسترسی غیرمجاز
- جلوگیری از حرکت جانبی مهاجم در شبکه
- مانیتورینگ و پاسخ به رخدادها
- پشتیبان گیری و تداوم کسب و کار

چالش ها / تهدیدات

- حملات اینترنتی (Brute Force, Exploit, DDoS)
- فیشینگ و مهندسی اجتماعی
- بدافزار و باج افزار
- تهدیدات داخلی و دسترسی بیش از حد
- نشت اطلاعات
- خرابی تجهیزات و از دسترس خارج شدن سرویس ها



راهنمای نمادها

اینترنت — کلاینت — فایروال / روتر
سیستم امنیتی — تلفن تحت شبکه — سوئیچ لایه ۳
دسترسی بی سیم — سرور

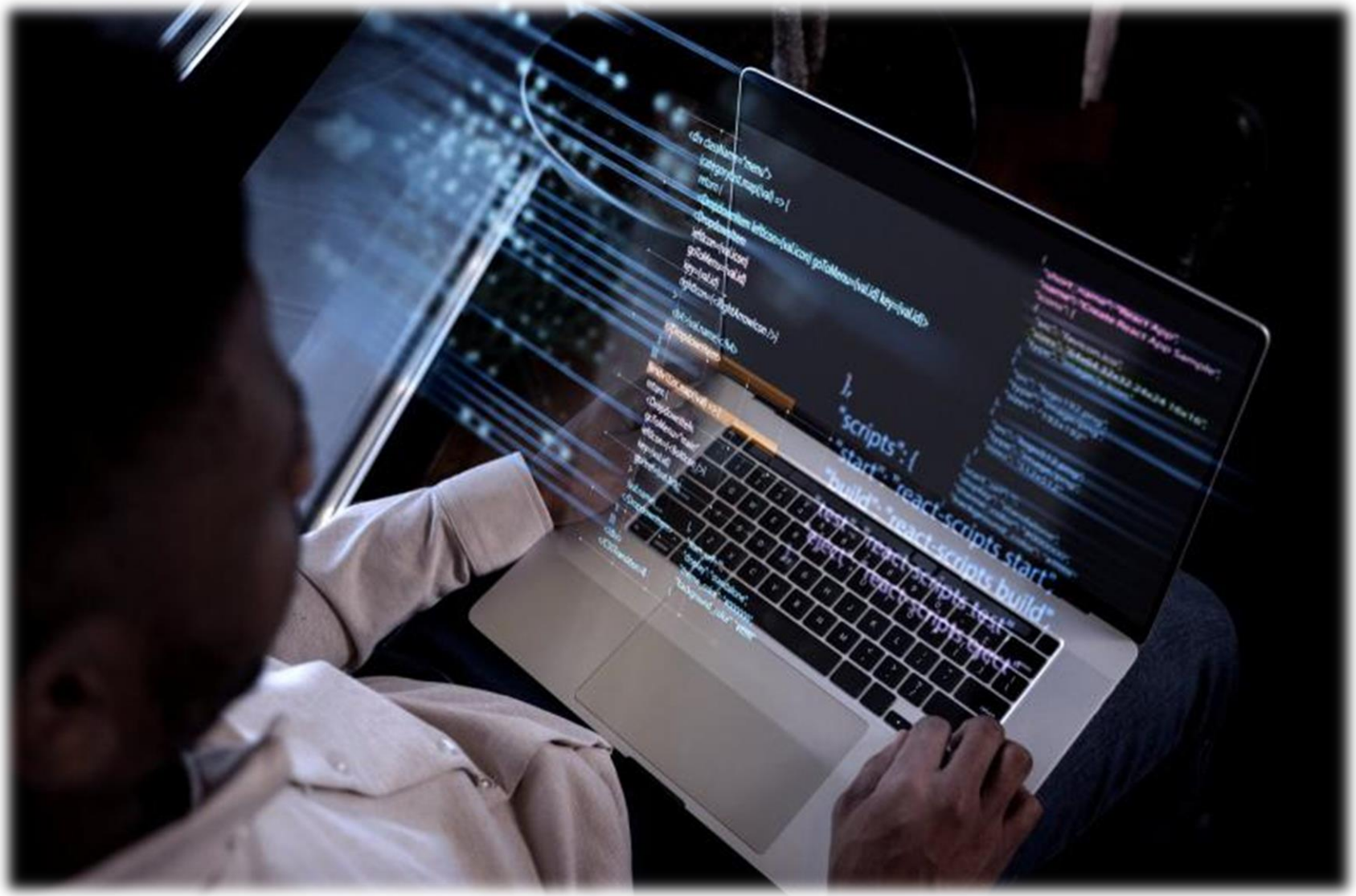
نکات طراحی امنیتی (Defense in Depth)

- لایه محیطی: فایروال, IDS/IPS, Anti-DDoS, WAF
- لایه شبکه: تقسیم بندی VLAN, Private VLAN, Private VLAN Security
- لایه سیستم: هاردنینگ سررورها و کلاینت ها، بروزرسانی Patch Management
- لایه هویت و دسترسی: Mtive Directory Security, Least Privilege Security
- لایه مانیتورینگ: جمع آوری و تحلیل لاگ ها در SIEM
- لایه داده: رمزنگاری: DLP, Backup منظم
- لایه پنجم پاسخ: Incident Response Plan و تمرین دوره ای

جدول آدرس دهی

VLAN	Network	Gateway	Description
10	10.0.10.0/24	10.0.10.1	Management
20	10.0.20.0/24	10.0.20.1	Users
30	10.0.30.0/24	10.0.30.1	Servers
40	10.0.40.0/24	10.0.40.1	VoIP
50	10.0.50.0/24	10.0.50.1	Guest
60	10.0.60.0/24	10.0.60.1	Virtualization/Backup
DMZ	10.10.10.0/24	10.10.10.1	DMZ Zone

مدل بلوغ امنیت تهاجمی



- مدل بلوغ امنیت تهاجمی به عنوان کسی که در حوزه امنیت تهاجمی(آفنسیو) فعالیت میکنید باید در نظر بگیرید هر سازمان یک ردیف بودجه ای میتواند به امنیت اختصاص دهد و شما با توجه به آن باید سعی به افزایش سطح امنیت بکنید.

- این مدل در واقع از پایین ترین سطح تا بالاترین سطح با توجه به بودجه سازمان می تواند تاثیر گذار باشد.

- تست نفوذ شامل اجرای قدم های موارد زیر هست که فقط مرحله دوم با دو مورد اول یکسان هست و پنتستر در واقع کارش اکسپلویت کردن تمام آسیب پذیری های کشف شده و ارزیابی شرایط بعد از اکسپلویت و در واقع میزان نفوذ پذیری به سازمان می باشد .

- information gathering
- enumeration and vulnerability scanning
- exploiting
- maintain access
- privilege escalation
- post exploitation
- reporting

ابزارهای برای گزارش نویسی پروژه تست نفوذ

- LaTeX
- Markdown
- G Suite or Microsoft Office 365
- visio
- microsoft word
- xmind

- حملات به چهار دسته عمده تقسیم می شوند:فعال، غیرفعال، مخرب و غیر مخرب.رایج ترین
- حملات در شبکه عبارتند از :

نام حمله	نوع حمله	محدوده استفاده	شرح حمله
جلوگیری از سرویس (DOS)	فعال	توسط کاربر داخلی و یا خارجی	کاربر نمی تواند از منابع و اطلاعات و ارتباطات استفاده کند
استراق سمع	غیرفعال	توسط کاربر داخلی و یا خارجی	مهاجم بدون اطلاع طرفین تبادل داده، به شنود پیام ها و اطلاعات می پردازد
تحلیل ترافیک	غیرفعال	اکثراً توسط کاربران خارجی	مهاجم ترافیک شبکه را تحلیل کرده و اطلاعات ارزشمندی را کسب می کند

دستکاری پیام ها و داده ها	فعال	معمولاً توسط کاربران خارجی	مهاجم جامعیت و صحت اطلاعات را با تغییرات غیرمجاز بهم می زند
جعل هویت	فعال	توسط کاربران خارجی	مهاجم هویت یک فرد مجاز در شبکه را جعل می کند

- نصب نرم افزار را محدود کنید
- وقتی آزادی نصب نرم افزار را به کاربران می دهید ، ممکن است برنامه های ناخواسته را نصب کنند که سیستم شما را به خطر بیاندازد. معمولاً سرپرست سیستم مجبور است تعمیر و نگهداری و تمیز کردن چنین سیستمهایی را انجام دهد. توصیه می شود از طریق گروپ پالسی، از نصب نرم افزار جلوگیری کنید:
- Computer Configuration>Policies> Administrative Templates> Windows Component> Windows Installer
- در بخش سمت راست صفحه، روی پالسی Prohibit User Installدبل کلیک کنید.
- برای فعال کردن پالسی روی Enableکلیک کنید.

Group Policy Management Editor

File Action View Help

- Text Input
- Windows Calendar
- Windows Color System
- Windows Customer Experience Imp
- Windows Defender Antivirus
- Windows Defender Exploit Guard
- Windows Defender SmartScreen
- Windows Error Reporting
- Windows Hello for Business
- Windows Ink Workspace
- Windows Installer
- Windows Logon Options
- Windows Media Digital Rights Mar
- Windows Media Player
- Windows Messenger
- Windows Mobility Center
- Windows PowerShell
- Windows Reliability Analysis
- Windows Remote Management (W
- Windows Remote Shell
- Windows Security
- Windows Update
- Work Folders
- All Settings

Windows Installer

Prohibit User Installs

Edit policy setting

Requirements:
Microsoft Windows XP or Windows 2000 with Windows Installer v2.0

Description:
This policy setting allows you to configure user installs. To configure this policy setting, set it to enabled and use the drop-down list to select the behavior you want.

If you do not configure this policy setting, or if the policy setting is enabled and "Allow User Installs" is selected, the installer allows and makes use of products that are installed per user, and products that are installed per computer. If the installer finds a per-user install of an application, this hides a per-computer installation of that same

Setting	State
Allow users to browse for source while elevated	Not configured
Allow users to use media source while elevated	Not configured
Allow users to patch elevated products	Not configured
Always install with elevated privileges	Not configured
Prohibit use of Restart Manager	Not configured
Remove browse dialog box for new source	Not configured
Prohibit flyweight patching	Not configured
Turn off logging via package settings	Not configured
Turn off Windows Installer	Not configured
Prevent users from using Windows Installer to install update...	Not configured
Prohibit rollback	Not configured
Turn off shared components	Not configured
Allow user control over installs	Not configured
Specify the types of events Windows Installer records in its tr...	Not configured
Prohibit non-administrators from applying vendor signed u...	Not configured
Prohibit removal of updates	Not configured
Turn off creation of System Restore checkpoints	Not configured
Prohibit User Installs	Not configured
Enforce upgrade component rules	Not configured

Extended Standard

22 setting(s)

- حالت تایید UAC برای سطح دسترسی Admin سیستم باید فعال باشد .
- UAC - User Account Control یک مکانیزم امنیتی براي محدود کردن افزایش سطح دسترسی

شامل حساب هاي کاربري با دسترسی administrativeاست، مگر اینکه مجاز باشد. این تنظیمات براي حساب هاي کاربري Administratorسیستمی پیکربندي میشوند بطوري که تحت حالت تایید Adminاجرا شوند

Windows Settings -> Security Settings -> Local Policies -> Security Options -> "**User Account Control: Admin Approval Mode for the Built-in Administrator account**" to "**Enabled**".

Group Policy Management

File Ac

Group Policy Management Editor

File Action View Help

Group Po

Fores

D

Si

G

G

- Computer Configuration
  - Policies
    - Software Settings
    - Windows Settings
      - Name Resolution Policy
      - Scripts (Startup/Shutdown)
      - Deployed Printers
      - Security Settings
        - Account Policies
        - Local Policies
          - Audit Policy
          - User Rights Assignmer
          - Security Options
        - Event Log
        - Restricted Groups
        - System Services
        - Registry
        - File System
        - Wired Network (IEEE 802.3
        - Windows Defender Firewa
        - Network List Manager Pol
        - Wireless Network (IEEE 80
        - Public Key Policies
        - Software Restriction Polic

Policy	Policy Setting
Network security: Restrict NTLM: NTLM authentication in this domain	Not Defined
Network security: Restrict NTLM: Outgoing NTLM traffic to remote servers	Not Defined
Recovery console: Allow automatic administrative logon	Not Defined
Recovery console: Allow floppy copy and access to all drives and all folders	Not Defined
Shutdown: Allow system to be shut down without having to log on	Not Defined
Shutdown: Clear virtual memory pagefile	Not Defined
System cryptography: Force strong key protection for user keys stored on the co...	Not Defined
System cryptography: Use FIPS compliant algorithms for encryption, hashing, a...	Not Defined
System objects: Require case insensitivity for non-Windows subsystems	Not Defined
System objects: Strengthen default permissions of internal system objects (e.g. S...	Not Defined
System settings: Optional subsystems	Not Defined
System settings: Use Certificate Rules on Windows Executables for Software Rest...	Not Defined
User Account Control: Admin Approval Mode for the Built-in Administrator acc...	Not Defined
User Account Control: Allow UIAccess applications to prompt for elevation with...	Not Defined
User Account Control: Behavior of the elevation prompt for administrators in Ad...	Not Defined
User Account Control: Behavior of the elevation prompt for standard users	Not Defined
User Account Control: Detect application installations and prompt for elevation	Not Defined
User Account Control: Only elevate executables that are signed and validated	Not Defined
User Account Control: Only elevate UIAccess applications that are installed in se...	Not Defined
User Account Control: Run all administrators in Admin Approval Mode	Not Defined
User Account Control: Switch to the secure desktop when prompting for elevati...	Not Defined
User Account Control: Virtualize file and registry write failures to per-user locatio...	Not Defined

خطراتی که باز کردن یک لینک شما را تهدید می کند

- هر کدام از ما هر روز چندین لینک را بدون اینکه بدانیم چه چیزی است باز می کنیم و این می تواند خیلی خطرناک باشد. مهمترین خطراتی که ممکن است با باز کردن یک لینک در معرض آن قرار بگیرید را بررسی میکنیم.

- **احتمال هک شدن از طریق لینک!**
- **نرم‌افزارهای مخرب (Malware):** لینک‌های مخرب ممکن است به نرم‌افزارهای ضررآور یا ویروس‌ها منجر شوند که به سیستم شما وارد شده و اطلاعات حساس را دزدیده یا سیستم شما را دچار مشکل کنند.
- **فیشینگ (Phishing):** لینک‌های فیشینگ تلاش می‌کنند اطلاعات حساس شما را مثل رمزعبورها و اطلاعات حساب بانکی خود را جمع آوری کنند. این لینک‌ها به طور کلی به نظر می‌رسند که از منابع قابل اعتمادی می‌آیند، اما در واقع توسط مهاجمان ایجاد شده‌اند.
- **هویت‌سرقت (Identity Theft):** لینک‌های مخرب ممکن است به منظور دسترسی به اطلاعات شخصی شما و سوءاستفاده از هویت شما ایجاد شوند.

- **هجمه‌های سایبری** :(**Cyber Attacks**) باز کردن لینک‌های مخرب ممکن است به سایر حملات سایبری مانند حملات دی.داس (DDoS)یا نفوذ به سیستم‌ها منجر شود.

- **جاسوسی** :(**Spyware**) لینک‌های مخرب ممکن است نرم‌افزارهای جاسوسی را بر روی سیستم شما نصب کنند و اطلاعات شخصی شما را جمع‌آوری کنند.

- **کد اجراپذیر** :(**Executable Code**) لینک‌هایی که کد اجراپذیر (executable code)را دارند ممکن است به اجرای کدهای مخرب بر روی سیستم شما منجر شوند.

- هکر امکان دارد یک همچین کدی را داخل هاست خود با فرمت html آپلود کرده باشد و لینک آن را به شما بدهد.

```
<iframe src="http://admin:admin@192.168.1.1/rebootinfo.cgi" width=0 height=0>
```

- اگر دقت کنید این کد داخل خود یک آیپی آشنا دارد(۱۹۲،۱۶۸،۱،۱) که همه با آن اشنا هستیم. این آیپی معمولا متعلق به صفحه کانفیگ مودم ها می باشد.

- کلمه های admin:admin را هم مشاهده می کنید که اولی به یوزر و دومی به پسورد پیشفرض مودم ها اشاره دارد در ادامه نیز کد دستور ریست کردن مودم وجود دارد.

- که در کل شما با لمس لینک آماده شده ابتدا به صورت خودکار وارد کانفیگ مودم خود می شوید و مودم خود را ریست می کنید.

- یک هکر میتواند تمام اکسپلویت های مربوط به مرورگرها را جمع آوری بکند و تمامی انها را داخل یک سایت جعلی به صورت طعمه هایی قرار دهد و لینک سایت جعلی (fake)خود را به تارگت بدهد.
- در این حالت تارگت در بین طعمه های جذاب گیر خواهد کرد و حتما به تور هکر گیر خواهد کرد. که در این صورت اگر ورژن مرورگر تارگت آسیب پذیر باشد، دسترسی لازم برای هکر ایجاد میشود.

Backup

- در سال‌های اخیر، Backup دیگر فقط «کپی گرفتن از اطلاعات» نیست؛ بلکه بخشی از استراتژی **Cyber Resilience** سازمان محسوب می‌شود.

- با افزایش حملات باج‌افزاری، خرابکاری داخلی، حذف تصادفی داده‌ها و حملات به زیرساخت‌های مجازی، سازمان‌ها به سمت معماری‌های پیشرفته‌تر Backup و Recovery حرکت کرده‌اند.

CYBER
RESILIENCE

Cyber Resilience(تاب‌آوری سایبری) یکی از مهم‌ترین مفاهیم امنیت سایبری در سال‌های اخیر است.
در گذشته هدف امنیت اطلاعات این بود که:
»از نفوذ جلوگیری کنیم«.

اما امروزه سازمان‌ها پذیرفته‌اند که:
»ممکن است روزی نفوذ یا حمله موفق اتفاق بیفتد؛ بنابراین باید بتوانیم سریع بازیابی شویم و کسب‌وکار را ادامه دهیم«.

- به همین دلیل مفهوم Cyber Resilienceشکل گرفت.
- تعریف ساده
- Cyber Resilienceیعنی:
- توانایی سازمان برای پیشگیری، شناسایی، پاسخ و بازیابی سریع از حملات سایبری بدون توقف جدی کسب‌وکار.

- **چهار ستون اصلی Cyber Resilience**
- **1. Prevent (پیشگیری)**
- کاهش احتمال حمله
- **نمونه‌ها:**

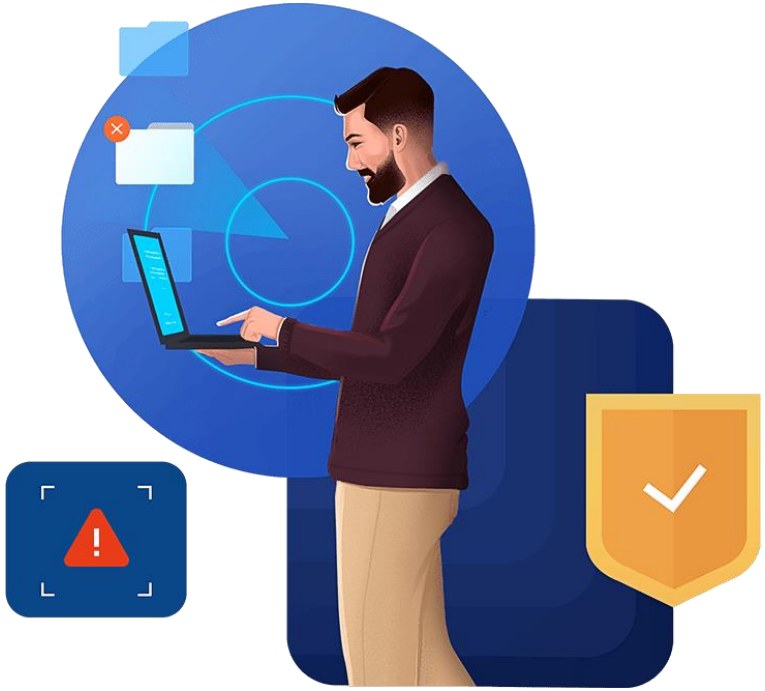
- Firewall
- EDR/XDR
- MFA
- Network Segmentation
- Hardening

- **2. Detect(تشخیص)**
- شناسایی سریع حمله
- نمونه‌ها:
- SIEM
- SOC
- Log Monitoring
- Threat Hunting

- **3. Respond (پاسخ)**
- کنترل و مهار حادثه
- نمونه‌ها:
- Incident Response
- Isolation
- Containment
- Forensics

- **Recover(بازیابی)**
- بازگشت سریع به شرایط عادی
- نمونه‌ها:
- Backup
- Disaster Recovery
- Business Continuity

Cyber Security	Cyber Resilience
تمرکز بر جلوگیری از حمله	تمرکز بر ادامه فعالیت پس از حمله
دفاع محور	بقا محور
امنیت تجهیزات	امنیت کسب‌وکار
جلوگیری از نفوذ	بازیابی پس از نفوذ



- **مثال واقعی**
- فرض کنید یک شرکت تولیدی به باج‌افزار آلوده می‌شود.
- **سازمان بدون Cyber Resilience**
- فایل‌ها رمزگذاری می‌شوند.
- Backupنیز آلوده شده است.
- تولید متوقف می‌شود.
- چند هفته اختلال.

- **سازمان دارای Cyber Resilience**
- حمله شناسایی می‌شود.
- شبکه آلوده ایزوله می‌شود.
- Backup Immutable موجود است.
- سرویس‌ها ظرف چند ساعت بازیابی می‌شوند.
- خسارت به حداقل می‌رسد.

ادامه جدیدترین متدهای پشتیبان گیری اطلاعات در سال 2026

- **رویکرد Cyber Resilient Backup**
- جدیدترین نگرش در دنیا:
- **هدف:** اطمینان از بازیابی سرویس حتی پس از حمله سایبری.
- **اجزای اصلی**
- Backupچندلایه
- Backupآفلاین
- تست دوره‌ای بازیابی
- مانیتورینگ رفتار فایل‌ها
- تشخیص رمزگذاری غیرعادی اطلاعات

مزیت

حتی در صورت آلوده شدن کل شبکه به Ransomware، نسخه Backupسالم باقی می‌ماند.

- **قانون 3-2-1-1-0**
- نسخه تکامل یافته قانون معروف Backup
- **3**
- سه نسخه از داده
- **2**
- ذخیره روی دو رسانه متفاوت
- **1**
- یک نسخه خارج از سایت
- **1**
- یک نسخه Offline
- **0**
- صفر خطا در تست بازیابی
- **مثال**
- Data Centerاصلی
- NAS Backup
- Cloud Storage
- **Immutable Storage**

Immutable Storage

- **Immutable Storage** به معنی فضای ذخیره‌سازی غیرقابل تغییر است.
- **به زبان ساده:وقتی** یک فایل Backup در Immutable Storage ذخیره شد، تا پایان مدت زمان تعیین‌شده هیچ شخص، نرم‌افزار، مدیر سیستم یا حتی باج‌افزار نمی‌تواند آن را حذف، ویرایش یا رمزگذاری کند.

- **مثال ساده**
- **فرض کنید از سرور مالی سازمان Backupگرفته‌اید.**
- در حالت عادی:
- Administratorمی‌تواند Backupرا حذف کند.
- مهاجم در صورت دسترسی ادمین می‌تواند Backupرا پاک کند.
- باج‌افزار ممکن است فایل‌های Backupرا رمزگذاری کند.
- **اما در Immutable Storage:**
- Deleteامکان‌پذیر نیست.
- Modifyامکان‌پذیر نیست.
- Encryptامکان‌پذیر نیست.
- فایل فقط خواندنی (Read Only)است.

- **چرا مهم است؟**
- امروزه اولین هدف بسیاری از باج‌افزارها Backupاست.
- مهاجم ابتدا:

1. Backup Serverرا پیدا می‌کند.
2. Snapshotها را حذف می‌کند.
3. Backupها را پاک می‌کند.
4. سپس فایل‌های اصلی را رمزگذاری می‌کند.

- **اگر Backupها Immutable باشند، حتی با دسترسی Administrator نیز مهاجم نمی‌تواند آن‌ها را حذف کند.**

معروف ترین محصولات برای این موضوع

- محصولات معروف
- Veeam Backup & Replication
- Rubrik
- Cohesity
- Commvault

- **در پروژه‌های سازمانی**
- وقتی در پروپوزال می‌نویسیم:
- **Cyber Resilient Backup Solution**
- معمولاً شامل موارد زیر است:
- Immutable Backup
- Air-Gapped Backup
- Backup Encryption
- Multi-Factor Authentication
- Backup Monitoring
- Recovery Testing
- Disaster Recovery Planning
- به همین دلیل امروزه در استانداردهای امنیتی جدید، **داشتن Backup به‌تنهایی کافی نیست**؛ بلکه داشتن **Immutable Backup** یکی از مهم‌ترین الزامات مقابله با حملات باج‌افزاری محسوب می‌شود.

- **Immutable Backup**
- یکی از مهم‌ترین تکنولوژی‌های روز دنیا
- **مفهوم**
- پس از ذخیره شدن Backup:
- حذف نمی‌شود
- تغییر نمی‌کند
- رمزگذاری نمی‌شود
- حتی Administratorنیز نمی‌تواند آن را تغییر دهد.
- **فناوری‌ها**

- Object Lock
- WORM Storage
- Hardened Repository

- **محصولات مطرح**

- Veeam Backup & Replication
- Commvault
- Rubrik
- Cohesity

- **Air-Gapped Backup**
- **تعریف**
- نسخه Backupکاملاً از شبکه جدا می‌شود.
- مثال:
- Tape Library
- Offline Disk
- Vault Storage
- **مزایا**
- باج‌افزار به آن دسترسی ندارد.
- **کاربرد**
- بانک‌ها
- صنایع نفت و گاز
- زیرساخت‌های حیاتی
- مراکز داده دولتی

- **Cloud Backup Architecture**
- امروزه بسیاری از سازمان‌ها به سمت Hybrid Backup رفته‌اند.
- **معماری**

- Primary Site
  ↓
  Local Backup
  ↓
  Cloud Backup

- **مزایا**
- Disaster Recovery
- نگهداری طولانی مدت
- کاهش هزینه تجهیزات
- **سرویس‌ها**

- Amazon Web Services
- Microsoft
- Google

- **Backup for Virtual Infrastructure**
- برای محیط‌های مجازی:
- **VMware**
- Image Level Backup
- CBT
- Instant Recovery
- **Hyper-V**
- Host Level Backup
- VM Replication
- **مزیت**
- بازیابی کامل ماشین مجازی در چند دقیقه.

- **Continuous Data Protection (CDP)**
- پیشرفته‌ترین روش Backup
- **شیوه کار**
- هر تغییر در فایل‌ها ثبت می‌شود.
- **قابلیت**
- بازگشت به:
- ساعت 10:05
- ساعت 10:10
- ساعت 10:15
- و نه فقط Backup شب گذشته.
- **کاربرد**
- ERP
- مالی
- بانکداری
- سامانه‌های حساس

- **CDP (Continuous Data Protection)** است، این یکی از پیشرفته‌ترین مدل‌های حفاظت از داده محسوب می‌شود.
- **CDP چیست؟**
- در Backup سنتی:

- 08:00 PM → Backup
- 08:00 PM → Backup روز بعد

- اگر ساعت 15:00 سرور خراب شود، اطلاعات بین 08:00 شب گذشته تا 15:00 امروز از دست می‌رود.

- اما در CDP:

- 10:01
- 10:02
- 10:03
- 10:04
- 10:05

- هر تغییر در داده‌ها به صورت پیوسته ثبت می‌شود.
- بنابراین می‌توانید سیستم را به هر لحظه دلخواه برگردانید.

- **مدل فنی CDP چگونه کار می‌کند؟**
- **روش اول: Block-Level Change Tracking**
- سیستم فقط بلوک‌های تغییر یافته را ذخیره می‌کند.
- **مثلاً**
- **Database 500 GB**
- فقط 10 MB تغییر کرده است.
- CDP فقط همان 10 MB را ذخیره می‌کند.
- مزایا:
- مصرف کم فضا
- سرعت بالا
- Recovery سریع

تفاوت Backup سنتی و CDP

ویژگی	Backupسنتی	CDP
RPO	ساعت‌ها	چند ثانیه
از دست رفتن داده	زیاد	بسیار کم
تعداد Restore Point	محدود	بسیار زیاد
هزینه	کمتر	بیشتر
پیچیدگی	کم	زیاد

- محصولات مطرح

- Veeam Backup & Replication
- Zerto
- Dell RecoverPoint
- VMware Site Recovery Manager

- **آیا همه سازمان‌ها به CDP نیاز دارند؟**
- **خیر.**
- برای اکثر شرکت‌ها ترکیب زیر کافی است:
- Immutable Backup
- Backup روزانه
- Replication
- Disaster Recovery

- اما برای سازمان‌هایی که **RPO نزدیک به صفر** نیاز دارند (بانک‌ها، بورس، پرداخت الکترونیک، مراکز داده حیاتی)، CDP ارزش بالایی دارد.

- **از دید یک مشاوره پروژه امنیت اگر بخوام بگم :**
- امروزه سازمان‌ها بیشتر به سمت این مدل حرکت می‌کنند:

Immutable Backup

+

Replication

+

Disaster Recovery Site

+

Cyber Resilience

زیرا نسبت به **CDP** هزینه کمتر و بازگشت سرمایه بهتری دارد، در حالی که همچنان مقاومت بالایی در برابر باج‌افزار و خرابی زیرساخت فراهم می‌کند.

- **Backup Security Assessment**
- امروزه سازمان‌ها تنها Backupنمی‌گیرند.
- Backup Security Auditانجام می‌دهند.
- **موارد بررسی**
- رمزنگاری Backup
- MFA
- دسترسی اپراتورها
- سلامت Backup
- قابلیت Recovery
- مقاومت در برابر Ransomware
- بررسی Retention Policy

- **Backup Policyاستاندارد سازمانی**
- **سطح 1 - داده‌های حیاتی**
- **نمونه**
- ERP
- مالی
- Active Directory
- Database
- **سیاست**
- Backupروزانه
- Backupهفتگی
- Backupماهانه
- نگهداری 1 تا 7 سال

- **سطح ۲ – داده‌های عملیاتی**
- **نمونه**
- File Server
- اتوماسیون
- CRM
- **سیاست**
- Backupروزانه
- نگهداری 6 ماه تا 1 سال

- **سطح ۳ – داده‌های عمومی**
- **نمونه**
- آرشیوها
- فایل‌های قدیمی
- **سیاست**
- Backupهفتگی
- نگهداری 3 تا 6 ماه

شاخص‌های مهم Backup Policy

- **RPO**
- حداکثر میزان اطلاعاتی که قابل از دست رفتن است.
- مثال:
- RPO = 15 Minutes

- **RTO**
- حداکثر زمان بازیابی سرویس.
- مثال:
- RTO = 1 Hour

- RPO و RTO را معمولاً **محاسبه نمی‌کنند، بلکه بر اساس نیاز کسب‌وکار تعیین می‌کنند** و سپس زیرساخت Backupرا طوری طراحی می‌کنند که به آن اعداد برسد.

- این یکی از اشتباهات رایج در بسیاری از پروژه‌هاست که ابتدا Backup تهیه می‌شود و بعد می‌پرسند RPO و RTO چقدر است؛ در حالی که باید برعکس باشد.

- **RPOچیست؟**
- **Recovery Point Objective**
- حداکثر میزان اطلاعاتی که سازمان حاضر است از دست بدهد.
- **مثال**
- فرض کنید:
- Backup هر ۲۴ ساعت یکبار گرفته می‌شود.
- ساعت ۱۴:۰۰ سرور خراب می‌شود.
- آخرین Backupساعت ۰۰:۰۰ بوده است.

- در این حالت:
- 14 ساعت اطلاعات از دست رفته است

- بنابراین:
- RPO = 24 Hours

- RPO ≈ فاصله زمانی بین دو Backup

RPO	نوع Backup
24 ساعت	روزانه
12 ساعت	هر 12 ساعت
1 ساعت	هر 1 ساعت
چند ثانیه	CDP

- **RTOچیست؟**
- **Recovery Time Objective**
- حداکثر زمانی که سازمان برای بازگرداندن سرویس به حالت عملیاتی می‌پذیرد.

- **مثال**
  - سرور SQLخراب می‌شود.
  - مدت زمان:
  - تشخیص خرابی: ۲۰ دقیقه
  - آماده‌سازی سرور: ۴۰ دقیقه
  - Restore Backup: 1ساعت
  - تست سرویس: ۳۰ دقیقه
- RTO = 2 ساعت و 30 دقیقه

نمونه واقعی در سازمان

Active Directory

اگر Domain از کار بیفتد:

مدیر سازمان می‌گوید:

حداکثر ۴ ساعت قطعی قابل قبول است

. RTO = 4 Hours

- **سیستم مالی**

مدیر مالی می‌گوید:

حداکثر ۳۰ دقیقه اطلاعات از دست برود.

- **روش تعیین RPO و RTO در پروژه**

گام ۱: شناسایی سرویس‌ها

مثلاً:

- Active Directory
- ERP
- SQL
- File Server
- Exchange

- **گام 2: تحلیل اثرات کسب‌وکار (BIA)**
- Business Impact Analysis
- سؤال می‌کنیم:
- اگر سرویس از کار بیفتد:
- چند ساعت قابل تحمل است؟
- چند دقیقه داده قابل از دست رفتن است؟

سرویس	RPO	RTO
Active Directory	1 ساعت	4 ساعت
SQLمالی	15 دقیقه	1 ساعت
ERP	30 دقیقه	2 ساعت
File Server	4 ساعت	8 ساعت
آرشیو	24 ساعت	48 ساعت

یک مثال عملی

- **فرض کنید شرکت شما:**
- ۱۰۰ کاربر
- ERPمالی
- SQL Server
- VMware
- **و مدیریت اعلام می‌کند:**

- حداکثر داده از دست رفته:
- **۳۰ دقیقه**

- **حداکثر زمان قطعی:**
- ۲ ساعت

- RPO = 30 Minutes
  RTO = 2 Hours
- برای رسیدن به این اهداف معمولاً معماری زیر پیشنهاد می‌شود:

- VMware
- │
- ▼
- Veeam Backup
- │
- ├─ Hourly Incremental
- │
- ├─ Immutable Repository
- │
- └─ Replication

خدمات قابل ارائه به مشتریان

- **Backup Assessment**
- بررسی وضعیت موجود
- تحلیل ریسک
- **Backup Architecture Design**
- طراحی ساختار Backup
- **Cyber Resilient Backup**
- طراحی مقاوم در برابر Ransomware
- **Disaster Recovery Planning**
- طراحی سناریوی بحران

- **Backup Policy Development**
- تدوین سیاست‌های Backup
- **Backup Hardening**
- امن‌سازی سرورها و مخازن Backup
- **Recovery Drill**
- تست دوره‌ای بازیابی
- **Backup Security Audit**
- ممیزی امنیتی Backup