Cybersecurity

Inhaltsverzeichnis

Definition - Cybersecurity

- Schutz von Netzwerken, Computergeräten, Daten und Diensten

- Netzwerk- & Anwendungssicherheit,
  Disaster Recovery, Endbenutzeraufklärung und kritische Infrastruktursicherheit

- Bedeutung auf Grund hoher Kosten und Folgen einer Datenschutzverletzung für Unternehmen und Kunden

Zero Days

- Neu entdeckte, nicht behobene Sicherheitslücken
- Nutzung zum Verbreiten von Malware oder Diebstahl von Daten
- Zero-Day-Angriff: Ausnutzung eines Zero-Day-Exploits, um Schaden anzurichten oder Zugriff zum System zu erlangen
- Gefährlich, da sie unerkannt bleiben und es keine bekannten Abwehrmaßnahmen gibt

Shodan

- Veröffentlichung in 2009
- Auffinden von Geräten im Internet
- Erfinder: John Matherly
- Name wegen Künstlicher Intelligenz aus System-Shock
- Nutzung verschiedener Filter zum Suchen
- Suche der Geräte über 8 Ports

Shodan Filter

- Insgesamt 81 Filter
- Country="DE"
- City="Cologne"
- Has_Screenshot="true"
- Has_IPV6="true"
- Ip="..."

Shodan Protokolle

- HTTP/HTTPS (80,8080,443,8443)
- FTP (21)
- SSH (22)
- Telnet (23)
- SNMP (161)
- SIP (5060)
- RTSP (554)

Splunk

- Gründung: 2003
- "Splunk" bezieht sich auf "spelunking"
- Log-, Monitoring-, Reporting-Plattform
- Nutzung zum Benachrichtigen von Admins
- Verbindung z.b. viaTeams möglich
- Gratis Alternativen: Grafana, Prometheus

Sniffing

Abhören von Netzwerkdatenverkehr

Durch Tools oder Software

z.B: Wireshark

Zwecke des Sniffing:

Analyse des Datenverkehrs und Netzwerklast

Überwachung für bösartige Zwecke z.B: DDoS, …

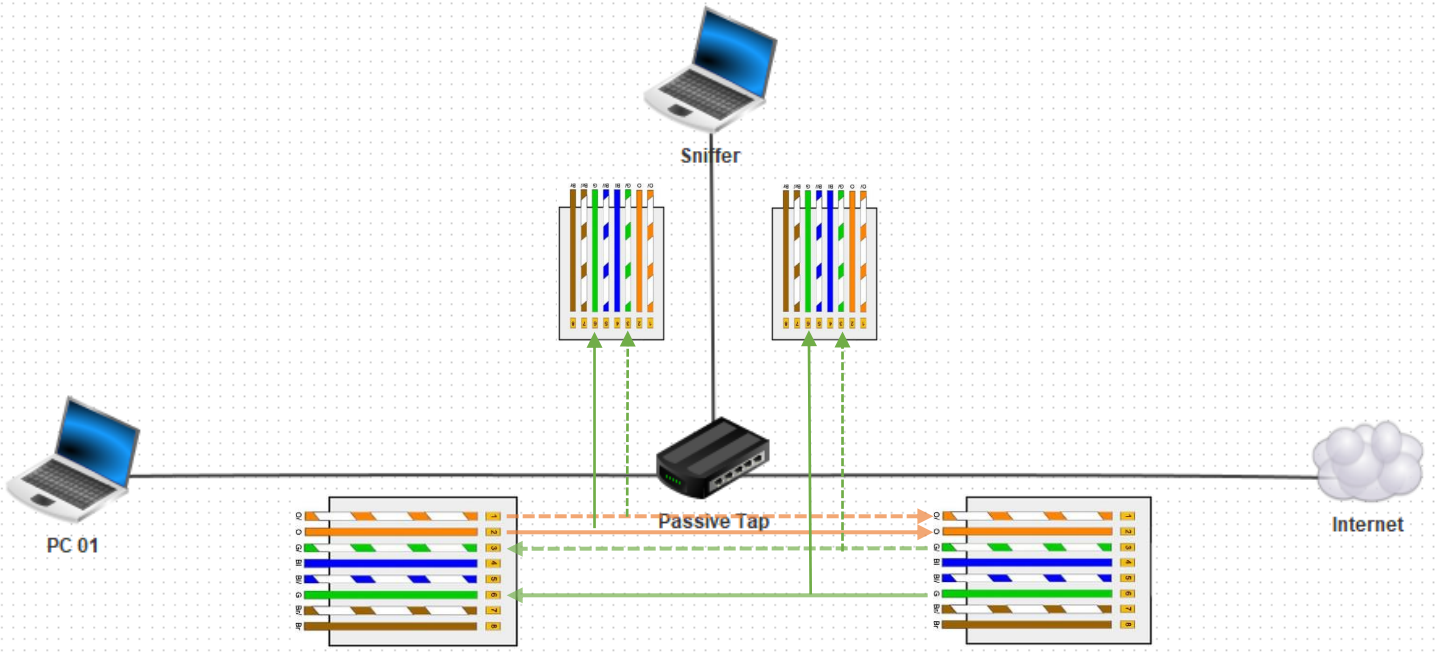
Passive LAN Tap

Datenverkehr zwischen PC01 und Internet

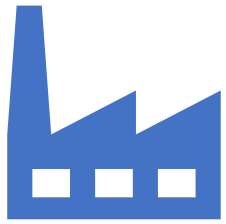
Richtung	LAN-Farbe
OUT	1. Orange/weiß 2. Orange
IN	3. Grün/weiß 6. Grün

Datenverkehr zwischen PC01 und Internet mit Sniffing

Sniffing-Tap	Verbunden mit:
IN: 3. Grün/Weiß 6. Grün	OUT: 1. Orange/Weiß 2. Orange
IN: 3. Grün/Weiß 6. Grün	IN: 3. Grün/Weiß 6. Grün



MikroTik Router



MikroTik lettischer Hersteller von Netzwerkgeräten und –software

Hauptprodukt ist Router OS

Stellt auch Router und Switches her

MikroTik vs Router

- MikroTik: fortschrittliche Funktionen
- hohe Konfigurierbarkeit
- MikroTiks: sicherer als herkömmliche Router
- Herkömmliche Router: benutzerfreundlicher
- MikroTiks: komplexer

MikroTik OS

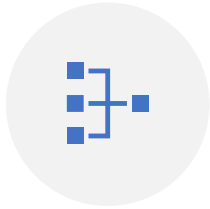
FIREWALL

VPN

HOTSPOT

ROUTING-PROTOKOLLE

QUALITY OF SERVICE (QOS)



NAT (NETWORK ADDRESS TRANSLATION)

Vorteile

Skalierbarkeit

Flexibilität

Sicherheit

Leistung

Ende

Quellen

https://alternativeto.net/software/splunk/?license=free

https://de.wikipedia.org/wiki/Splunk

https://www.kaspersky.de/resource-center/definitions/zero-day-exploit

https://www.computerbild.de/artikel/cb-Tipps-Sicherheit-Was-ist-ein-Zero-Day-Exploit-33413091.html

https://www.welivesecurity.com/deutsch/2015/03/17/sicherheitsbegriffe-erklart-bedeutet-zero-day/

https://de.wikipedia.org/wiki/Shodan

https://www.splunk.com/de_de

https://www.shodan.io/

https://www.shodan.io/search/filters