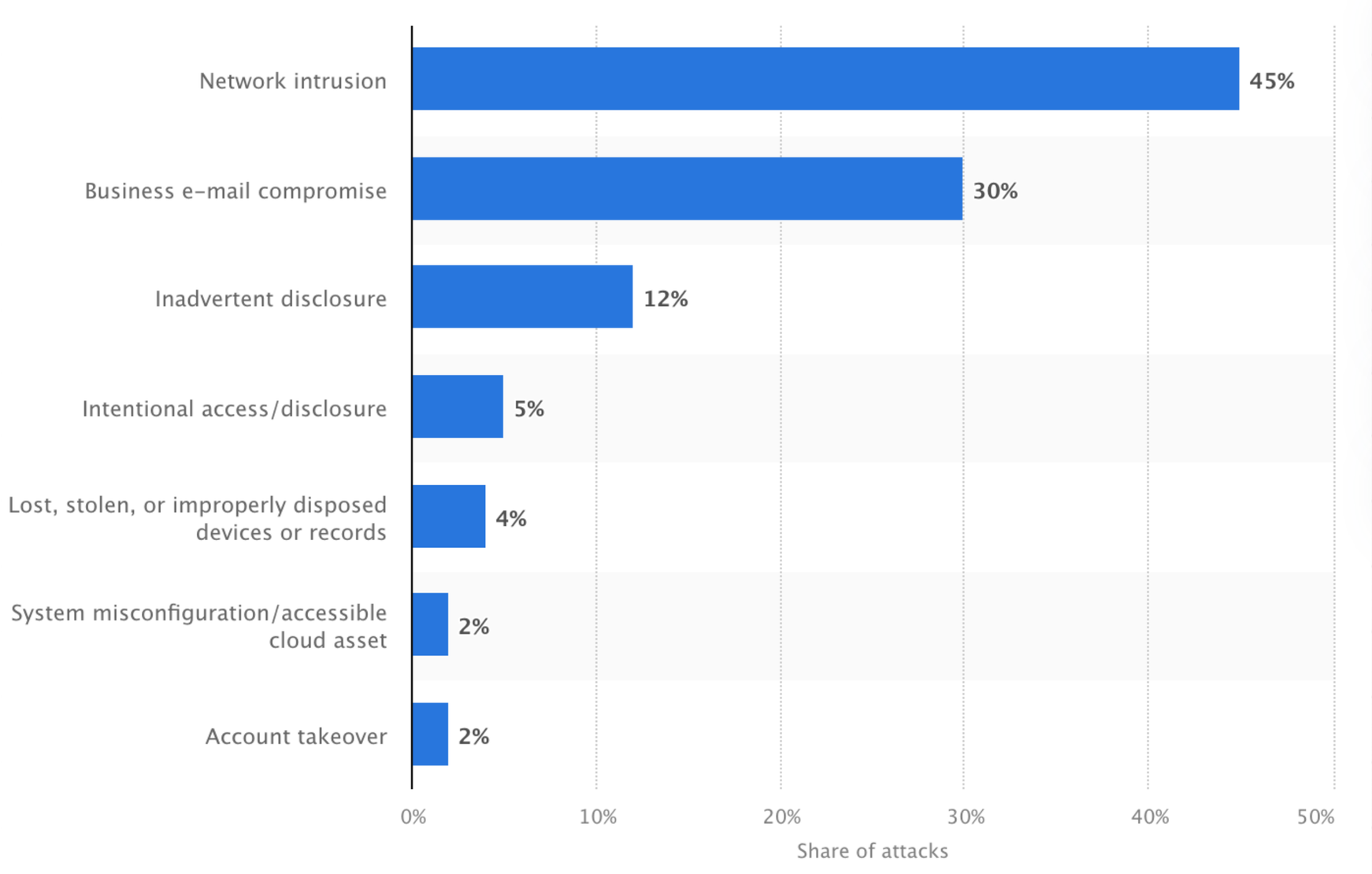
UNMASKING THE UNINVITED:

AN EXPLORATION OF COMBATING UNAUTHORIZED NETWORK ACCESS

HAVE YOU EVER DEALT WITH UNAUTHORIZED NETWORK ACCESS OR SCARED THAT YOUR COMPUTER MAY BE NEXT??!

NETWORK INTRUSIONS ARE THE MAIN CULPRIT



MOST COMMON TYPES OF CYBER ATTACKS EXPERIENCED BY COMPANIES IN THE U.S. 2022

SOURCE: STATISTA.COM

THESE CAN HELP YOU!

RISK MITIGATION STRATEGIES

NETWORK SCANNER

- Scans devices on network
- Detects vulnerabilities
- Allows administrators do their job
- Security holes get fixed before they get exploited

FIREWALL

- Barrier between the inside and outside of network
- Monitors incoming and outgoing network traffic
- Analyzes each packet of data
- Prevents attackers from gaining entry

RISK MITIGATION STRATEGIES 2

WIFI SCANNER

- Detect network interferences
- Perform regular Scans
- Identify rogue access points
- Discover hidden SSIDs

WIFI SCANNER

Product Options

- Software based WIFI Scanners
  - Kismet and Netspot
- Hardware based WIFI Scanners
  - TP-Link Archer T2U Plus
  - Alfa AWUSO36ACH

Setup Time

- Kismet can range from a few hours to a day or more depending on factors such as familiarity with the system, complexity of the network environment

Setup Cost

- Open source software and affordable hardware using rasberry PI boards.
- Some software tools with advanced features may cost from around $20-$200

Maintenance Outlook

1. Vendor support and community engagement
2. Backups and recovery of configuration, databases, and critical data

Maintenance Cost

- Hardware maintenance like warranty, repairs and upgrades
- Software updates and supports like free software and subscipton services

Important Considerations

1. Scan coverage and depth
2. Scalability, speed and performance

NETWORK SCANNER

Product Options

- Tenable Security Center (Nessus)
  - Ideal for large enterprises
- Rapid7 Nexpose
  - Ideal for SMB's

Setup Time

- Nexpose takes approximately 15 days to install and configure, depending on the complexity of the network

Setup Cost

- Hardware cost to run Nexpose varies. Can run on AWS.
- No network downtime, but may cost take 15 days of IT wages

Maintenance Outlook

- Rapid7 has favorable reviews for their UI and support staff
- Being software-based, Nexpose won't require EOL hardware upgrades

Maintenance Cost

- Expect to spend ~10% of IT budget on cybersecurity
- $20-25/yr per asset. e.g. $6500/yr for 250 network assets

Important Considerations

- Nexpose is an ideal choice because of its intuitive UI, excellent customer support, and leading updates to their CVE list and identification technology

NEXTGEN FIREWALL

Product Options

- Palo Alto
  - Ideal for large enterprises
- Fortinet FortiGate
  - Ideal for SMB's

Setup Time

- Installation may take several days depending on complexity of network and user base

Setup Cost

- FortiGate hardware costs $1,000-$4,000 for SMB's.
- Installation downtime may cause revenue loss

Maintenance Outlook

- FortiGate has leading UI and customer support which reduces maintenance and downtime

Maintenance Cost

- Expect to spend ~10% of IT budget on cybersecurity
- FortiGate licenses cost ~50% of hardware cost per year
- Hardware upgrade every 5 years

Important Considerations

- NGFW's are preferred over traditional firewalls because they combine several security technologies into one platform to combat the latest attack vectors

CREATING A NETWORK SCANNER

What it is and how it works

A network scanner is a software tool that scans the network for connected devices. Here's how it works:

- The sending device sends an ARP Request containing the IP Address of the device it wants to communicate with.
- After receiving the broadcast message, the device with the IP address equal to the IP address in the message will send an ARP response containing its MAC address to the sender.

Implementing the network scanner

In my python script, I will follow these steps to design the network scanner:

- Creating an arp request packet which has the target IP address.
- Send packet to the broadcast and receive a response from the target IP address.
- parse the response to get the Mac
- print result

Creating a network scanner using Scapy Library in Python

main.py

```python
from scapy.all import ARP, Ether, srp
#crafting packets
target_ip = "192.168.1.1/24"
#IP address for the destination
#Create ARP Packet
arp = ARP(pdst = target_ip)
#creating the ethernet broadcast packet
ether = Ether(dst = "ff:ff:ff:ff:ff:ff")
#stack them
packet = ether/arp
result = srp(packet, timeout=3, verbose=0)[0]

# a list of clients, we will fill this in the upcoming loop
clients = []

for sent, received in result:
    # for each response, append ip and mac address to `clients` list
    clients.append({'ip': received.psrc, 'mac': received.hwsrc})

# print clients
print("Available devices in the network:")
print("IP" + " "*18+"MAC")
for client in clients:
    print("{:16}    {}".format(client['ip'], client['mac']))
```

```
Available devices in the network:
IP                  MAC
192.168.1.1         e8:94:f6:c4:97:3f
192.168.1.119       ec:1f:72:26:a9:a5
```

CREATING A NETWORK FIREWALL PT1

Network Design

- Cable modem for internet access
- Internal LAN with workstations, home file server,
- Public wireless network separated on DMZ network

Hardware Setup

- Devil Linux is a 'live' distribution, runs directly from CD-ROM
- Configuration stored on a separate disk (floppy drive or USB thumb drive)
- PC needs a CD-ROM drive, no hard drive required

Make the CD

- Download Devil Linux stable release
- Unzip the downloaded file
- Find and burn the bootcd.iso file to a CD using suitable software

Boot-up:

- -Connect monitor and keyboard
- Insert boot CD and power up
- Watch for the boot screen, and system will automatically boot

Login:

-Enter 'root' as the username
Press enter for the password
Type 'setup' and press enter to access the setup menu

CREATING A NETWORK FIREWALL PT2

Congifiguration:

- Navigate setup menu (arrow keys, spacebar)
- Configure basics (hostname, timezone)
- Enable/disable network services (e.g., SSHD, NAMED)

Firewall Configuration:

- Choose DMZ3FW or FW2 in Networking menu based on NICs
- Install basic firewall rules (select 'yes')

Network Setup

- Configure NICs in Networking menu. (NICs stands for Network Interface Cards
- Set modules for each NIC
- Configure IP for eth0 (internet-facing NIC)
- Set DHCP for local NICs if needed

DHCP Configuration:

-Adjust DHCP settings in main menu option

THANK YOU VERY MUCH!