Übungsgruppe: Qianli Wang und Nazar Sopiha

Dyn cyberattack in 2016:

a)

1. **I) Authentizität (home routers, IP-Cameras, Baby-Monitors, u.s.w. werden als Botnets, also einzelne Einheiten während der Attack benutzt)**
   II) Verfügbarkeit (Viele sehr berühmte Webseiten, wie z.B. Amazon, Airbnb, Netflix u.s.w., für einige Zeit nicht verfügbar waren)

2. **Das war eine einfache, schon vorher bekannte DDoS-Attack, einfach mit einer ganz großen Menge der Devices, die gleichzeitig an das Web-Server angreifen. Man könnte die Kapazität des Web-Servers vergrößern, aber es ist nicht realistisch, Servers für so eine große Menge der Benutzer in einem Zeitpunkt zu unterstützen. Deswegen, außer Standardschutz der Webseiten von DDoS-Attacks, betreffen die Maßnahmen eher einzelne Benutzer und nicht das System.**

- **Sicherstellen, dass keine Standardkennwörter auf den Geräten belassen werden. Verwenden zuverlässige Kombinationen, die nicht einfach erzwungen werden können.**
- **Aktualisieren die Firmware für alle Geräte, insbesondere für die älteren.**
- **Seinen wählerisch bei der Auswahl smart device. Frag sich, ob nötig ist, mit Internet zu verbinden.**

Schutz von DDoS Attack von Server Seite:

- **Front-end Hardware anwenden**
- **Schlüssel Abschluss Indikatoren auf Anwendungsebene verwenden**
- **DDoS-orientierte Verteidigung**

3. **Große Kapazitäten für den Empfang und die Verarbeitung von Daten nicht verfügbar.**

   Diese Web Seiten waren sehr berühmt und für relativ viele Benutzer gleichzeitig gedacht, deswegen wurde eine unerwartet große Aktivität nicht sofort als etwas gefährliches anerkannt, sondern eher normal für

4. **<u>Methode des Eindringens:</u>**

   A distributed denial of service (DDoS) attack

<u>Ablauf des Angriffs:</u>

<u>Vorbereitung:</u>

I. **Hacker infizieren verschiedene Rechner im ganzen Internet**
II. **Verknüpfen sie zu einem Botnet**
III. **Zielen dann mit dem Botnet auf ein einziges Opfer ab.**
IV. **Systeme auf Schneckentempo verlangsamen und schließlich abstürzen lassen.**

3 Attacks: 7:00-9:20, 11:52, 16:00-18:11

5. **Was zunächst als Angeberei anfing, diente schon bald dazu, andere einzuschüchtern oder Leuten, die man nicht mehr ins Business sehen möchte, „eins auszuwischen“. Außerdem haben diese Attacken auch als Protestaktionen gedient.**

6. **Die Dyn-Angriffe wurden wahrscheinlich nicht von einem Staat veranlasst. Die Angreifer waren höchstwahrscheinlich Hacker, die auf Dyn wütend waren, weil das Unternehmen Brian Krebs bei der Identifizierung -- und das FBI bei der Verhaftung -- von zwei israelischen Hackern unterstützte, die einen Ring für auftragbare DDoS-Angriffe organisiert hatten. Die Angriffen richten sich gegen Internet-Infrastrukturunternehmen und scheinen von einem Nationalstaat auszugehen.**

7. **Software IT company Dynatrace monitors more than 150 websites, and found that 77 were impacted. The disruption may have lost companies up to $110 million in revenue and sales, according to CEO John van Siclen.**

b) DDoS Attack ist schon seit langem bekannt. Diese Attack war nach Einschätzungen 2 mal so stark wie die stärkste bisher gesehen. Wir glauben nicht, dass Web Seiten wie Netflix oder CNN waren nicht genug mit Standardschutz Methoden gegen DDoS gesichert, also dass wir jetzt neue Methoden (für diese Situation) finden können. Trotzdem machen wir einige hilfreiche Vorschläge:

1. **What to Look For In a DDoS Mitigation Service:**

It is beneficial to choose a DDoS mitigation service that keeps engineers and network administrators on site continuously monitoring traffic

2. **Businesses also need to understand equipment's capabilities to identify both network-layer and application-layer attacks. If there are not these resources in-house, then should work with ISP, data center, or security vendor to get advanced protection resources.**

Wir glauben, dass der Aufwand viel höher war, als den entstehenden Schaden, das kann aber auch geändert werden, falls Attacks wiederholt werden. Diese Angriffen können mehrmals wiederum passieren und wir wissen bisher nicht das echte Ziel der Hackers, also die haben ein sehr großes System für eventuelle weitere Angriffen gebaut und wir haben nur ein Anwendungsbeispiel davon betrachtet.

-- "I can't speak for anyone else, [But] I don't know that we really understand what the endgame is." © Joe Weiss, the managing partner at the cybersecurity firm Applied Control Solutions and the author of Protecting Industrial Control Systems from Electronic Threats.

Quellen:

https://www.kaspersky.com/blog/attack-on-dyn-explained/13325/

https://www.telekom.com/de/verantwortung/datenschutz-und-datensicherheit/magenta-security-kongress-2016/magenta-security-kongress-2016/lernen-aus-ddos-angriff-auf-dyn-444378

https://en.wikipedia.org/wiki/Denial-of-service_attack#Defense_techniques

https://en.wikipedia.org/wiki/2016_Dyn_cyberattack

https://money.cnn.com/2016/10/22/technology/cyberattack-dyn-ddos/index.html

https://phoenixnap.com/blog/prevent-ddos-attacks

https://www.theguardian.com/technology/2016/oct/26/ddos-attack-dyn-mirai-botnet