* + **1.Microsoft Azure (2021)**
* **Quy mô tấn công: 3.47 Tbps**, lớn nhất từng được ghi nhận.
* **Thời gian bị tấn công và khôi phục:** Kéo dài khoảng vài phút; không gây gián đoạn dịch vụ nhờ hệ thống giảm thiểu mạnh mẽ.
* **Phương thức:** Sử dụng kỹ thuật tấn công khuếch đại qua giao thức UDP từ nhiều nguồn để làm ngập lụt lưu lượng vào máy chủ Azure.
* **Tổn thất:** Không có thiệt hại tài chính hay gián đoạn lớn được báo cáo.
* **Cách khắc phục:** Microsoft triển khai lớp bảo vệ đám mây đa tầng và phân phối lưu lượng tấn công trên toàn cầu
  + **2. Google (2017)**
    - * **Quy mô tấn công: 2.54 Tbps (cao nhất lịch sử thời điểm đó).**
      * **Thời gian bị tấn công và khôi phục: Kéo dài hơn 6 tháng**; Google không để dịch vụ bị gián đoạn nhờ cơ sở hạ tầng mạnh mẽ.
      * **Phương thức:** Sử dụng 180.000 máy chủ CLDAP, DNS, và SMTP để gửi dữ liệu giả mạo với 167 triệu gói mỗi giây (Mpps). Cuộc tấn công được cho là do một nhóm hacker nhà nước ở Trung Quốc thực hiện.
      * **Tổn thất**: Google không công bố thiệt hại tài chính cụ thể nhưng sự kiện này làm tăng áp lực chi phí để cải thiện hệ thống bảo mật.
      * **Cách khắc phục:** Hệ thống phòng thủ toàn cầu với các công nghệ phát hiện sớm và giảm thiểu tự động giúp Google tránh thiệt hại lớn
  + **3. Amazon AWS (2020)**
    - * **Quy mô tấn công: 2.3 Tbps.**
      * **Thời gian bị tấn công và khôi phục:** Diễn ra trong một thời gian ngắn; AWS không công bố thời gian cụ thể nhưng giảm thiểu được mà không gây gián đoạn dịch vụ.
      * **Phương thức**: Sử dụng giao thức CLDAP để khuếch đại lưu lượng tấn công.
      * **Tổn thất:** Không có báo cáo về tổn thất tài chính, nhưng AWS đã phải chi thêm chi phí để duy trì lòng tin của khách hàng và cải thiện bảo mật.
      * **Cách khắc phục:** Hệ thống tự động phát hiện và phân phối lưu lượng tấn công đến các máy chủ dự phòng trên toàn cầu​

1. **Tỷ lệ tổ chức bị tấn công**:
   * Báo cáo từ **Cisco Annual Cybersecurity Report** cho thấy **1/3 các tổ chức đã từng bị tấn công DDoS**, với con số ngày càng tăng hàng năm.
   * Theo **Kaspersky Lab**, gần **50% các doanh nghiệp vừa và nhỏ (SME)** coi DDoS là một trong những mối đe dọa an ninh mạng lớn nhất.

* **1. Google (2017) – "Cơn ác mộng kéo dài"**

Đầu tiên, chúng ta nói về Google. Năm 2017, Google đối mặt với một cuộc tấn công DDoS có quy mô lên tới **2.54 Tbps**, lớn nhất vào thời điểm đó. Điều đáng sợ là cuộc tấn công kéo dài hơn **6 tháng**, với hàng trăm ngàn máy chủ bị lạm dụng để gửi dữ liệu giả mạo.

Cuộc tấn công này không làm Google gián đoạn dịch vụ, nhưng đây là lời cảnh tỉnh lớn vì nó được cho là do **một nhóm hacker nhà nước Trung Quốc** thực hiện. Google đã sử dụng hệ thống bảo mật toàn cầu để giảm thiểu lưu lượng độc hại, đồng thời cải thiện cơ sở hạ tầng sau sự kiện này.

* **2. Microsoft Azure (2021) – "Cuộc tấn công lớn nhất lịch sử"**

Tiếp theo là Microsoft Azure. Năm 2021, họ phải chịu một cuộc tấn công DDoS lớn nhất từng được ghi nhận, đạt **3.47 Tbps**. Tuy nhiên, nhờ hệ thống phòng thủ hiện đại, Microsoft chỉ mất **vài phút** để ngăn chặn cuộc tấn công này.

Cuộc tấn công sử dụng giao thức UDP để khuếch đại lưu lượng tấn công. Mặc dù không có tổn thất tài chính, Microsoft đã chứng minh được khả năng xử lý khủng hoảng hiệu quả, giúp củng cố niềm tin từ khách hàng.

* **3. Amazon AWS (2020) – "Hành động kịp thời"**

Cuối cùng là Amazon AWS. Họ đối mặt với một cuộc tấn công đạt đỉnh **2.3 Tbps** vào năm 2020. Thời gian tấn công không dài, nhưng mục tiêu rõ ràng là làm gián đoạn dịch vụ. AWS đã phản ứng nhanh, không để xảy ra tổn thất hay gián đoạn nghiêm trọng.

Cuộc tấn công sử dụng giao thức CLDAP để khuếch đại dữ liệu, nhưng nhờ hệ thống giảm thiểu tự động và mạng lưới máy chủ toàn cầu, Amazon đã giữ được sự ổn định cho khách hàng.

* **Bài học và Kết luận**

Qua ba trường hợp này, chúng ta thấy rằng dù là các công ty công nghệ hàng đầu thế giới, họ vẫn phải đối mặt với nguy cơ tấn công mạng cực lớn. Điểm chung của cả Google, Microsoft và Amazon là **khả năng ứng phó nhanh chóng** và **đầu tư mạnh vào hạ tầng bảo mật**. Điều này nhắc nhở tất cả chúng ta – nhất là những sinh viên CNTT – rằng an ninh mạng không chỉ là lý thuyết mà còn là một yếu tố sống còn.

1. **Mức độ sợ hãi trước DDoS**:
   * Cuộc tấn công DDoS thường làm gián đoạn dịch vụ, gây thiệt hại lớn về tài chính và uy tín, khiến các công ty trong lĩnh vực tài chính, thương mại điện tử, và công nghệ đặc biệt lo ngại.
   * **Verizon Data Breach Investigations Report** (DBIR) chỉ ra rằng DDoS chiếm gần **40% tổng số vụ tấn công mạng** trong một năm.
2. **Chi phí của các cuộc tấn công DDoS**:
   * Báo cáo từ **Cybersecurity Ventures** ước tính các cuộc tấn công DDoS gây thiệt hại trung bình khoảng **$120,000–$2 triệu USD** cho một công ty, tùy thuộc vào quy mô và thời gian gián đoạn.

**Lý do các công ty lo ngại:**

* **Khó dự đoán**: DDoS có thể xảy ra bất kỳ lúc nào, từ bất kỳ nguồn nào, mà không cần lý do cụ thể.
* **Dễ thực hiện**: Với các công cụ tấn công ngày càng phổ biến và chi phí thấp, DDoS trở thành vũ khí dễ tiếp cận cho các hacker.
* **Thiệt hại lớn**: Các cuộc tấn công có thể làm gián đoạn toàn bộ dịch vụ trực tuyến, làm giảm lòng tin khách hàng và gây mất doanh thu nghiêm trọng.

**Ngành nghề dễ bị tấn công:**

* **Thương mại điện tử**: Các doanh nghiệp như Amazon, eBay bị ảnh hưởng nặng nề nếu hệ thống ngừng hoạt động, dẫn đến mất doanh thu ngay lập tức.
* **Ngân hàng và tài chính**: Đây là mục tiêu hấp dẫn của hacker để gây hỗn loạn hoặc làm tê liệt hệ thống thanh toán.
* **Công nghệ và viễn thông**: Các công ty như Google, Microsoft và AWS thường xuyên đối mặt với các cuộc tấn công do hệ thống họ phục vụ hàng tỷ người dùng.

**Giải pháp bảo vệ:**

* **Sử dụng công cụ phòng chống DDoS**: Các dịch vụ như Cloudflare, Akamai, AWS Shield.
* **Phân phối hệ thống**: Dịch vụ đám mây giúp giảm tải hiệu quả khi bị tấn công.
* **Giám sát và phản ứng nhanh**: Xây dựng đội ngũ an ninh mạng để phát hiện sớm và xử lý các đợt tấn công.