The Top 10 Cyberattacks

Threatening Your Organization

Cybersecurity has never felt more complicated. With the number of threats growing at a rapid pace, IT staffs are struggling to protect every potential attack surface. While the number of specific bugs, viruses, bots, and exploits is beyond measure, they often fall within the same handful of attack types.

In this infographic, we take a look at the top 10 cyberattacks in today's evolving threat landscape. With this list, you can take the first steps to tighten your security strategy and ultimately keep your business ahead of any threats.

In 2018, **53%** of midmarket companies experienced a breach[1]

1 Phishing

Phishing is a malicious email that tricks users to surrender their user credentials. The email may appear legitimate, as if coming from your bank, and ask you to reset your password.

66% of malware is installed via malicious email attachments[2]

82% of manufacturers have experienced a phishing attack in the past year[3]

2 Malware

Malware is malicious software that spreads via an email attachment or a link to a malicious website. It infects the endpoints when a user opens the attachment or clicks on the link.

The average cost of a data breach in 2020 **$3,900,000**[4]

Over **75%** of the healthcare industry has been infected with malware over the last year[5]

3 Ransomware

Ransomware is a type of malicious software that prevents the end user from accessing a system or data. Attackers typically request a payment, often in the form of bitcoins, to decrypt files or restore access.

Ransomware costs businesses more than **$75B/year**[6]

Ransomware is predicted to cost **$6 trillion** annually by 2021[7]

4 DDoS

Distributed Denial-of-Service Attack

A distributed denial-of-service attack is an attack with the purpose of crashing a web server or an online service by flooding it with more traffic than it can handle.

There was a **967%** increase of DDoS attacks for 100Gbps or higher in Q1 2019[8]

DDoS attack frequency has increased more than **2.5X in 3 years**[9]

5 Brute-Force Password Attack

A brute-force attack is an attempt by a malicious actor to gain unauthorized access to secure systems by trying all possible passwords and guessing the correct one.

Today's tools can crack a single dictionary word password **within 1 second**[10]

80% of hacking-related breaches are caused by compromised, weak, and reused passwords[11]

6 Man-in-the-Middle Attack

Man-in-the middle attack is an attack where two legitimate users or devices are communicating with each other and have an undetected third-party secretly spying.

95% of HTTPS servers are vulnerable to MitM[12]

1/3 of exploitation of inadvertent weaknesses involved MitM attacks[13]

7 SQL Injection

An SQL injection exploit executes malicious SQL queries to take control of a database server that is running a web application.

98% of WordPress vulnerabilities are related to plugins that extend the functionality and features of a website or a blog[14]

59% of all websites using a known content management system use Wordpress[15]

8 Zero-Day Attacks

A zero-day attack takes place when hackers exploit a previously undisclosed vulnerability in hardware, software, or a network that has been exposed. Because the exploit is new, there is no remedy available.

76% of successful attacks on organization endpoints were zero-day attacks[16]

77.5 Average numbers of days to close a vulnerability[18]

9 Outdated and Unpatched Software

Companies often use older software that has reached end-of-life and is no longer receiving new patches, making the software vulnerable to any new exploits that are developed.

20% of all vulnerabilities caused by unpatched software are classified as High Risk or Critical[18]

60% of organizations that suffered a data breach within the last two years cited known vulnerabilities that hadn't been patched as the reason[19]

10 Insider Threats

Because insiders are already in your network and have some level of legitimate access, they have the time and capability to snoop around and steal data.

88% of companies with >1 million folders don't limit access[20]

The average cost of a malicious insider attack **rose 15%** from 2018 to 2019[21]

References

1. Cisco Cybersecurity Special Report, 2018
2. Verizon Data Breach Investigations Report (DBIR), 2017
3. Check Point 2018 Security Report
4. Security Cost of a Data Breach Report, 2019
5. Beazley Breach Briefing: Healthcare Industry Security Report
6. Datto, State of the Channel Ransomware Report 2018
7. Cybersecurity Ventures, Official Annual Cybercrime Report
8. Nexstar, Cyber Threats and Trends Report.
9. VPI Global Fraud and Mobile Traffic Forecasts, 2017
10. IBM Security, Verizon Data Breach Investigations Report (DBIR), 2016
11. Verizon Data Breach Investigations Report (DBIR), 2019
12. IBM, X-Force Threat Intelligence Index, 2018
13. Netcraft, 2016
14. Imperva, The State of Web Application Vulnerabilities in 2018
15. Imperva, The State of Web Application Vulnerabilities in 2018
16. Ponemon, 2018 State of Endpoint Security Risk
17. Scan, 2019 VULNERABILITY STATISTICS REPORT
18. Servicenow and Ponemon Institute, Costs and Consequences of Gaps in Vulnerability Response, 2018
19. Edgescan Stats Report, 2019
20. Varonis, Global Data Risk Report, 2018
21. Accenture and Ponemon, 2019 Cost of Cybercrime