radware

EUROPEAN APPLICATION & NETWORK SECURITY REPORT 2016-17

TABLE OF CONTENTS

EUROPEAN APPLICATION & NETWORK SECURITY REPORT 2016-17

01 INTRODUCTION

For six consecutive years, Radware has published its annual *Global Application & Network Security Report*. Through statistical research coupled with frontline experience, this research identifies trends that can help educate the security community. This year, for the first time, Radware introduces its findings to the European IT security community, focusing on the struggles that IT security professionals across Europe are facing to keep their organizations secured from lurking perils.

The study builds on prior years' research, collecting vendor-neutral information about issues that organizations faced while planning for and combating cyber-attacks. It provides a comprehensive review of 2016 cyber-attacks from both a business and a technical perspective and gives best practices for organizations to consider when planning for 2017. The report also reflects our Emergency Response Team's (ERT) in-the-trenches experiences fighting cyber-attacks and incorporates perspectives of two third-party service providers.

Radware's *European Application & Network Security Report* helps understanding the following:

1. The threat landscape—analysis of events, changes and trends
2. Potential impact on your business, including associated costs of different cyber-attacks
3. Easy steps to fortify your defense and be well prepared
4. Experiences of organizations in your industry
5. Predictions

This report offers a detailed review of:

- Known and common attacks of the past year (that is, what most people are attempting to secure against)
- Known and uncommon attacks (that is, what top performing organizations attempt to address—security incidents akin to the natural disasters cited above)
- Unknown attack forecast (that is, what has yet to demonstrate itself with evidence but is VERY "forecastable")

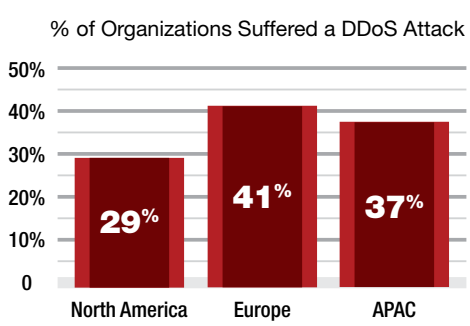
The quantitative data source is an industry-wide survey conducted by Radware. The survey had 157 individual respondents representing a wide variety of organizations across Europe. The study builds on prior years' research, collecting vendor-neutral information about issues that organizations faced while planning for and combating cyber-attacks.

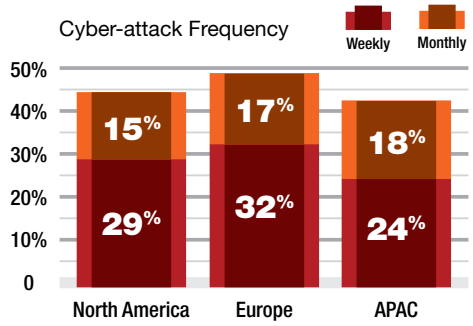
On average, responding organizations have an annual revenue of €1.7 billion and about 3,000 employees, and the profile ranges between SMBs (25% below 100 employees) to large enterprises (20% above 10,000 employees). Eighteen percent are large organizations with at least €1 billion in annual revenue. Respondents represent more than 12 industries, with the largest number coming from the following: carrier & telecommunications (25%), high tech products and services (17%), professional services & consulting (16%), and banking and financial services (11%). The survey provides balanced coverage between the different countries —with 16% of respondents coming from Spain, 13% from the United Kingdom, 12% from Italy, 11% from France, 10% from Germany and 38% from others. Additionally, 37% of the organizations conduct business worldwide, and 34% are multinational organizations across Europe.

EUROPEAN THREAT LANDSCAPE 02

The European IT security environment is very demanding. Each country has its own laws and regulations concerning privacy, confidential data, personal information and intellectual property, and so does the European Union. Businesses must invest resources in auditing, adapting and preparing to ascertain their compliance. In addition, many social, national and geopolitical conflicts can threaten organizations, such as state-sponsored cyber-attacks, attacks resulting from ideological and religious differences, espionage, and more.

During 2016, European business were attacked more frequently compared to other geographies. However, European IT security teams are lagging behind in the level and quality of protection strategies when compared to developments in the threat landscape, which eventually results in greater operational and financial losses.





Figures 1 & 2 – European organizations are attacked more

Global Report Highlights

98% of Organizations Experienced Attacks in 2016

Cyber-attacks became a way of life for nearly every organization in 2016. This trend will continue in 2017.

IoT Botnets Open the 1Tbps Floodgates

This exemplifies why preparing for "common" attacks is no longer enough. This event introduced sophisticated vectors, such as GRE floods and DNS water torture.

Cyber-Ransom Proves Easiest, Most Lucrative Tool for Cybercriminals

Almost all ransom events have a different attack vector, technique or angle. There are hundreds of encrypting malware types, many of which were developed and discovered this year as part of the hype. In addition, DDoS for ransom groups are professionals who leverage a set of network and application attacks to demonstrate their intentions and power.

Cyber-Attacks Cost Almost Twice What You May Think

Most companies have not come up with a precise calculation of the losses associated with a cyber-attack. Those who have quantified the losses estimate the damage at nearly double the amount compared to those who estimate.

Stateful Devices: #1 Point of Failure

Common IT devices, including firewalls, application delivery controllers and intrusion protection systems, now represent the greatest risk for an outage. Consequently, they require a dedicated attack mitigation solution to protect them.

European Highlights

Increased Attacks Against Civil-Service Organizations

2016 brought a new level of politically-affiliated cyber protests. Media reported on a different breach almost weekly. These incidents happened across the globe, with regimes suffering from cyber-attacks due to alleged corruption or perceived injustices. For example, concerns have risen in Europe about cyber security around the 2017 elections in France and in Germany.

As noted, European organizations tend to be attacked more, but are less prepared. European organizations suffered from the sophistication of new attack vectors and the prosperity of the cyber-attack-as-a-service market via the Darknet. An economic system has evolved in the Darknet where hackers and cyber criminals exchange practices and tools, where premium is paid for quality and competition drives the entry price to the minimum, thereby reducing the technical expertise required to execute an attack. Somebody can get a 20-minute 1Gbps DDoS attack for as low as €19.99. Consequently, there is a rise in the sophistication, prevalence and power of cyber-attacks, creating an imbalance where the investment load shifted towards the organizations.

Cyber Ransom #1 Motivation

According to half of European organizations

42% Suffered an SSL-based Attack

47% increase from 2015

Attacks Are More Frequent

1/2 are attacked monthly, 1/3 weekly

Availability & Data Are the Top Business Concerns

These are the main targets of hackers too

IoT Botnets Open the 1 Tbps Floodgates

58% of organizations feel IoT increases attack surface

Emerging Risks

In 2016, there was a marked increase in three principal attack types – cyber-ransom, encrypted and botnets based on IoT devices – which challenged traditional security models and forced businesses to rethink their posture looking forward.

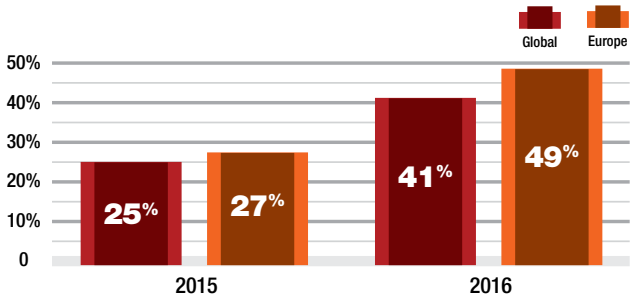


Figure 3: Financial / Ransom motives are behind cyber-attacks

Forms of SSL-Based Attacks

1. Encrypted SSL floods: Similar in nature to standard SYN flood attacks seeking to exhaust the resources expecting to complete a handshake. Encrypting the traffic complicates the challenge, forcing greater resource allocation.

2. SSL renegotiation: Initiating a regular SSL handshake and then immediately renegotiating the encryption key, repeatedly until all server resources are exhausted.

3. HTTPS floods: Generating floods of encrypted HTTP traffic. Compounding the impact of "normal" HTTPS floods, encrypted HTTP attacks add the burden of encryption and decryption mechanisms.

4. Encrypted Web application attacks: Multi-vector campaigns also increasingly leverage non-DoS, Web application logic attacks. By encrypting the traffic that masks these attacks, they often pass undetected through security controls.

Cyber-Ransom

Ransom is by far the number one motivation behind cyber-attacks, reported by 49% of European organizations – 20% higher than the global average. That shows a prevalence higher by 25% than the global benchmark of 41%. These ransom attacks came in two forms – malware or DDoS threats, both of which Radware's ERT faced multiple times during 2016 when customers were subjected to extortion attempts.

The second most popular motivation was espionage/competition – which affected 30% of European businesses surveyed. The good news is that only 10% of organizations could not indicate the motivation behind attacks they suffered. That most likely points to better visibility and awareness organizations have today.

Friend Turned Enemy: SSL-Based Cyber-Attacks

Increasingly, attackers are using the SSL protocol to mask and further complicate attack traffic and malware detection in both network and application-levels. Challenges posed by encrypted traffic are poised to get worse, as Gartner has noted: "The continued growth of SSL/TLS traffic will be amplified by adopting HTTP 2.0. It creates a new attack surface for malware infection, data exfiltration and call back communication."[1] According to Netcraft, use of SSL by the top one million websites has increased by more than 48% over the past two years.[2] As the percentage of inbound and outbound traffic increases, so does the effectiveness of encryption as a smokescreen for hackers. Recent surveys show that on average, 25% to 35% of enterprise communication sent through a LAN and WAN infrastructure is SSL-encrypted traffic.[3] In certain verticals, such as finance or medical, it can reach as high as 70% due to the information being communicated. SSL technology continues to improve the security it provides, with longer, more complex keys used to encrypt data.

1 "Security Leaders Must Address Threats From Rising SSL Traffic" Gartner Research, January 8, 2015
2 https://news.netcraft.com/archives/2014/01/03/january-2014-web-server-survey.html
3 http://www.networksasia.net/article/3-reasons-ssl-encryption-gives-false-sense-security.1424935771

SSL Attacks In Europe

SSL-based attacks against European organizations have grown 47% year-over-year, and 43% reported being hit by at least one in 2016 (vs. 29% in 2015). Unfortunately, only 23% of businesses confidently state they are capable of mitigating this type of attack, which clearly indicates a growing gap between the scope of the problem and the current level of preparedness. If this trend continues in 2017, there will be a larger gap which exposes financial institutions, ecommerce and many other businesses to SSL-based attacks. To prepare companies should think about how they can increase compute power, offload SSL traffic, avoid full inspection and defend from SSL-based attacks.

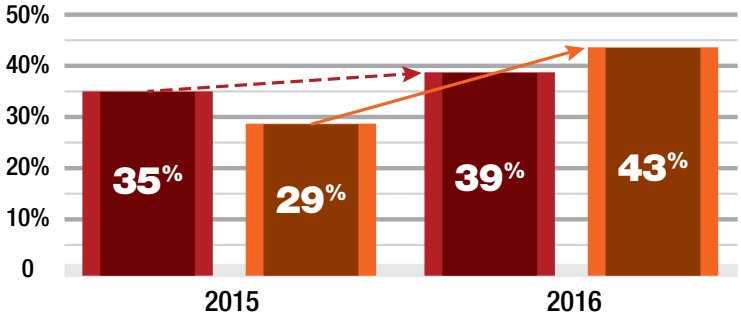


Figure 4: Rapid growth of SSL-based attacks against European organizations

IoT Botnets - Mirai Rewrites the Rules

2016 brought a long-feared DDoS threat to fruition: cyber-attacks were launched from multiple connected devices-turned-botnets. These attacks are propelling the industry into the 1Tbps DDoS era. What follows is a closer look at what happened—and what to do now.

As the first IoT open-source botnet, Mirai is changing the rules of real-time mitigation and making security automation a must. It is not just that IoT botnets can facilitate sophisticated L7 attack launches in high volumes. The fact that Mirai is open-source code means hackers can potentially mutate and customize it— resulting in an untold variety of new attack tools that can be detected only through intelligent automation.

The Mirai botnet struck the security industry in three massive DDoS attacks that shook traditional DDoS protection paradigms, proving that the Internet of Things (IoT) DDoS botnet threat is real and the grounds for building powerful and sophisticated cyber-attack tools.

In addition to generating traffic volumes above 1Tbps, Mirai features a selection of ten predefined attack vectors, some of which have proven effective in taking down the infrastructure of service providers and cloud scrubbers by attacking their protections. Among the ten vectors, there are highly sophisticated attack vectors such as GRE floods, TCP STOMP and Water Torture attacks. Mirai DDoS attacks also highlight the challenges organizations face when it comes to visibility into the legitimacy of GRE traffic or recursive DNS queries.

Radware's *2016-2017 Global Application and Network Security Report* features a complete study of the Mirai code, its attack vectors and possible enhancements.

Regulations in Cyber Security

Compliance is a big concern for European organizations as regulations change from one country to another and the EU standards are on top. Nevertheless, over 90% of security professionals think these requirements are fair to permissive, and only 8% perceive the regulation to be too strict. Less than 10% find current government policies too strict.

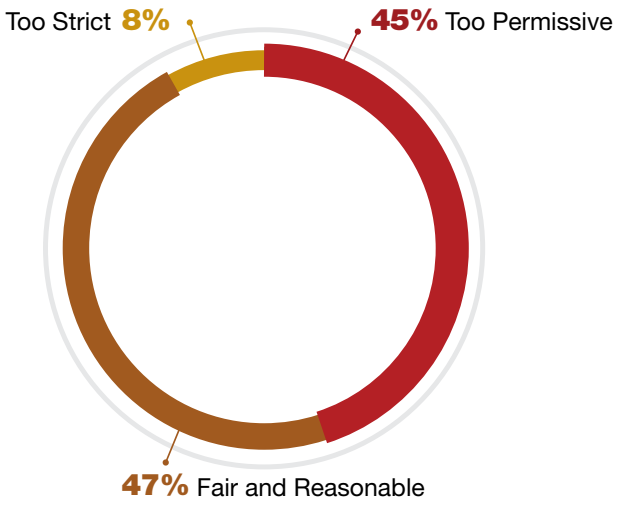


Figure 5: How do you find current government policies and regulation in the cyber security space?

03 ORGANIZATIONS IN EUROPE

Real Experiences

Attack Impact

Sixty-nine percent of security professionals in Europe say that either a partial or a full service degradation (complete outage) are the strongest drivers of a significant impact on an organization's infrastructure caused by a cyber-attack. In today's interconnected digital era, service degradation can negatively affect the end-user experience, followed by lower conversion rates, lower brand equity and significant financial losses. One in five responded that attacks had no impact on their infrastructure.

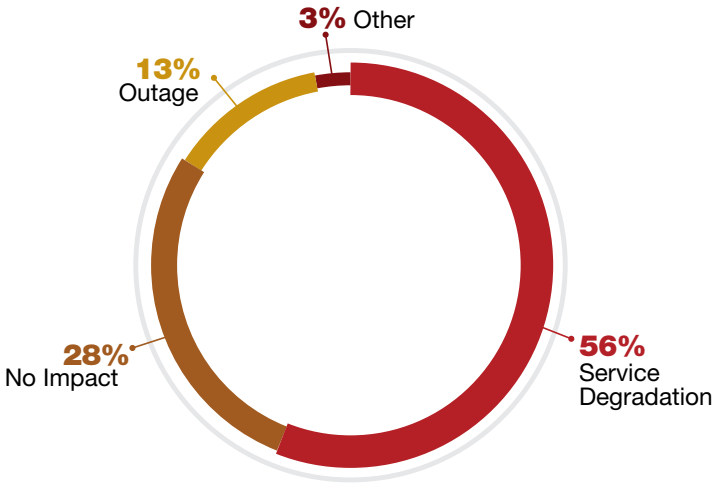


Figure 6: Typically, what is the impact of a cyber-attack on your infrastructure?

Network vs. Application Attacks

- Nearly 30% of survey respondents experience TCP-SYN Flood, ICMP, and UDP-Flood attacks on a weekly basis
- Layer 7 flood (HTTP, HTTPS) attacks have grown significantly
- One in three respondents suffered an attack against their DNS server weekly
- European organizations suffer more network/application attacks compared to the global average (69% and 67%, vs. 63% and 64%, respectively)

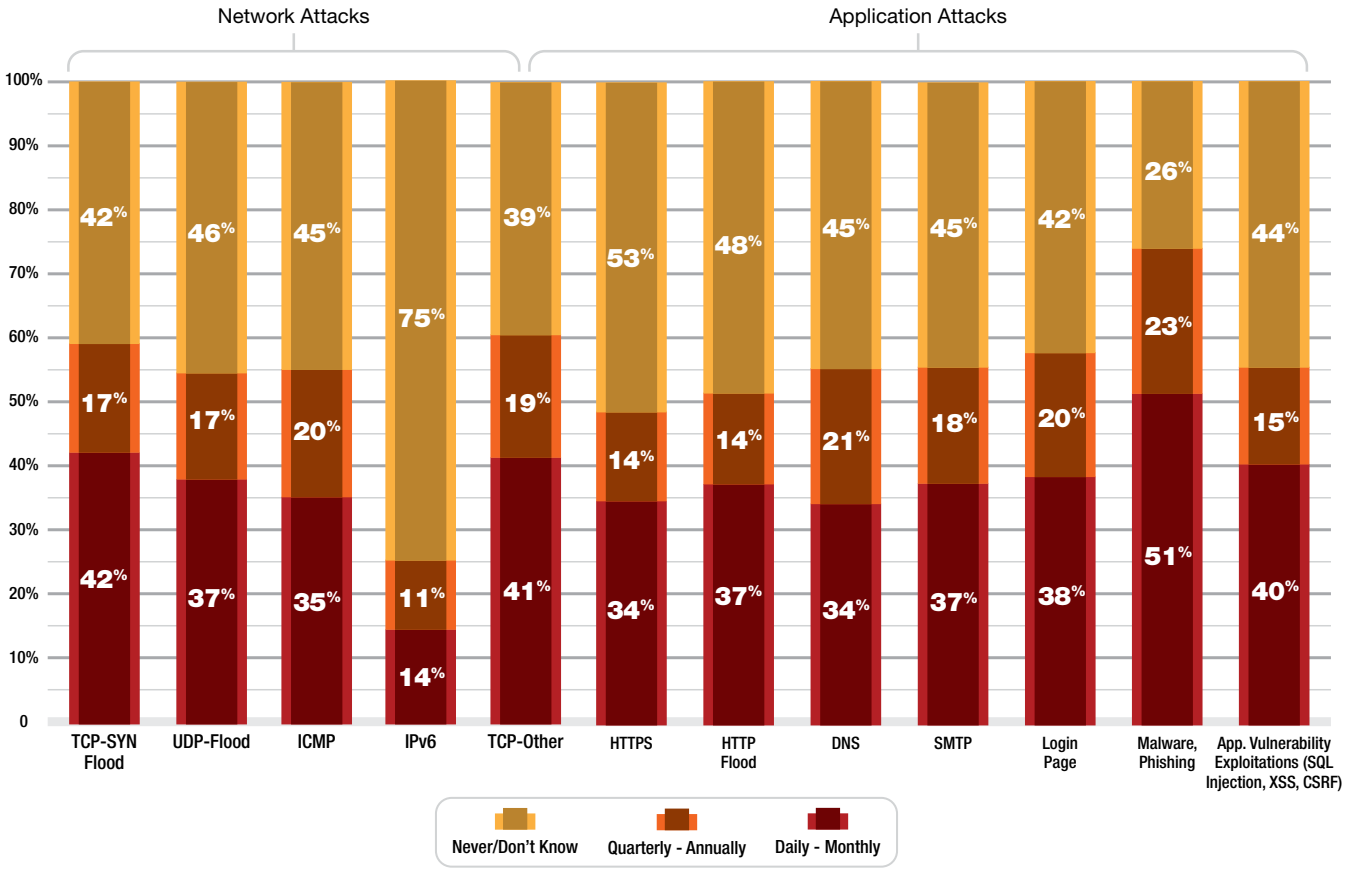


Figure 7: How often have you experienced the following attack in 2016?

Also, DDoS attacks are becoming shorter. In 2015, only 35% reported bursts lasting up to 3 hours; in 2016 this number grew to 48%.

Non-Volumetric DoS: Alive and Kicking

Despite the astonishing volumes of the headline-catchy IoT botnet attacks, neither the number of victims nor the frequency of attacks has grown. Seventy-six percent of European businesses suffer attacks in relatively low volumes (below 1Gbps), and 80% suffer attacks below 100Mbps. Rate-based security solutions continue to fall short, requiring companies to rethink their security strategy and embrace more sophisticated solutions. Without those upgrades, there is a good chance an organization will experience - yet lack the visibility – into service degradation.

Business Concerns

Service Availability is #1 Concern

In 2016, service availability (partial or full) and data loss were the top two concerns for European organizations – more than reputation loss or revenue loss. It corresponds well with the complex regulation around data protection in the different countries.

- 34% - partial/full availability impact or inability to meet SLA is the #1 concern
- 23% - data loss is the primary concern related to cyber activity, corresponds with global trend
- Fewer concerned with reputation loss and customer loss

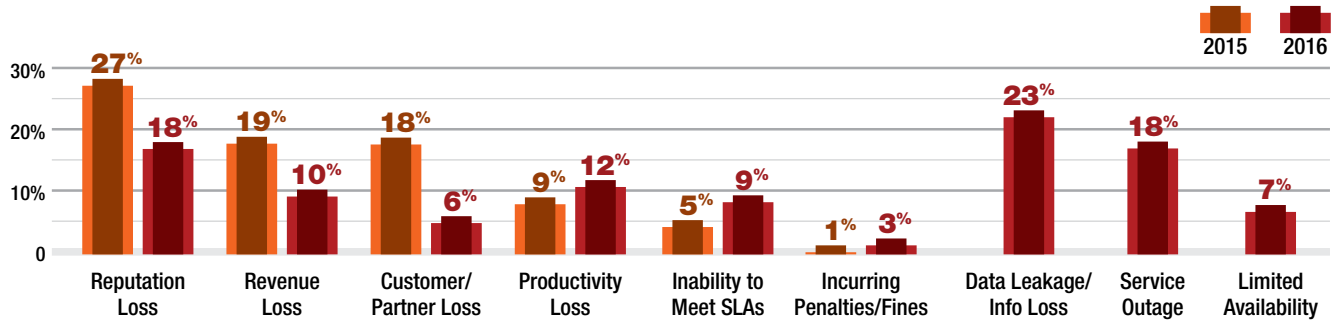


Figure 8: What are your business concerns if your organization is faced with a cyber-attack?

Failure Point Under DDoS Attacks

Businesses have shared their experiences about network failures caused by DDoS attacks. On one hand, the most targeted component is the server, which corresponds well with the perpetrators' intent of getting ahold of sensitive data. However, survey results show that in 36% of the cases, stateful devices are the component that fails, usually because their connection tables quickly filled out when large volumes of traffic hit. Moreover, for 25% of respondents, the Internet pipe becomes saturated, thereby rendering the network unreachable. Having a dedicated, stateless, DDoS mitigation solution at the perimeter, backed up by a cloud scrubbing service (a.k.a. hybrid DDoS protection), would mitigate the majority of these threats, reducing the number of network failures caused by DDoS attacks by up to 60%.

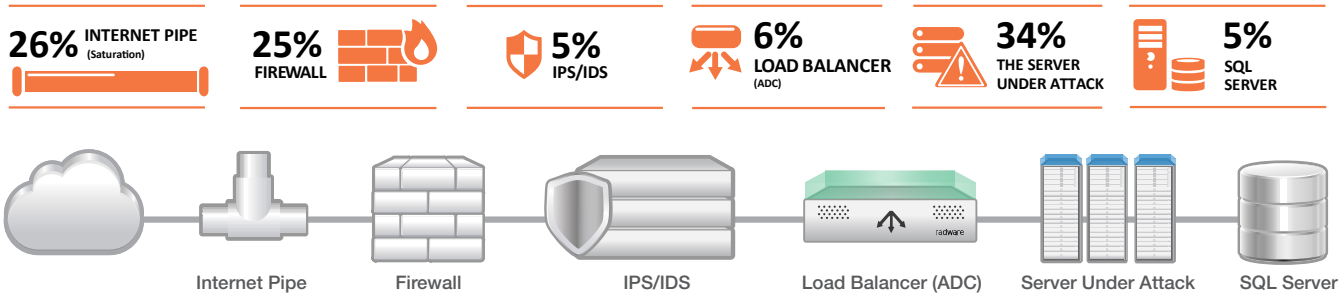


Figure 9: What are the three biggest cyber-attacks you have suffered: impact on?

Weakness Against DDoS Attacks

One in three organizations report their Internet links are not capable of withholding large volumetric DDoS attacks. Though this is a decline from 2015, it still represents a large portion of companies that have not yet chosen a cloud scrubbing solution for mitigation of such attacks. In addition, 29% see encrypted attacks as the vector they feel exposed to, corresponding with other findings on the prevalence of SSL-based attacks across the continent. About one-fourth feel vulnerable to attacks on their DNS servers. Low-and-Slow denial of service attacks seem to be concerning more and more organizations compared to 2015.

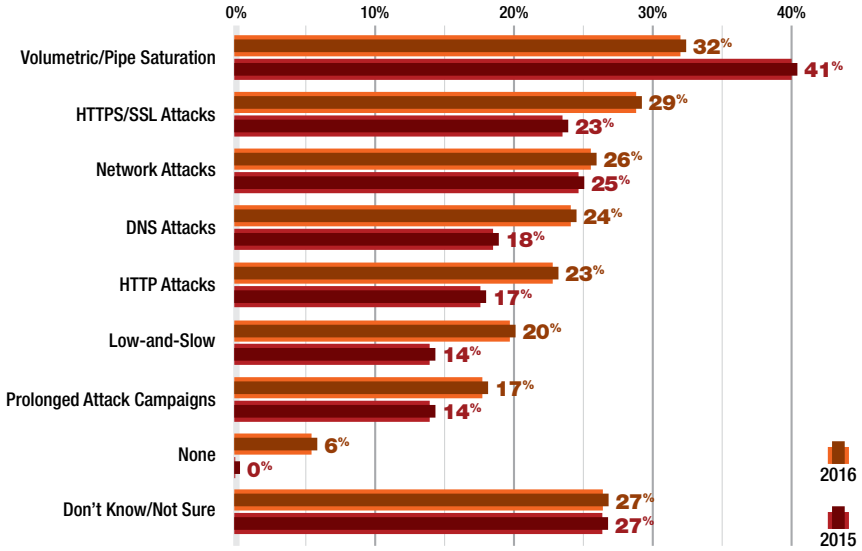


Figure 10: Where, if at all, do you think you have a weakness against DDoS attacks?

Chasm of Preparedness

Many organizations seem to be falling short when it comes to preparing for cyber-attacks. They are exposed when attacks are long and involve complex attack campaigns and many lack “the hacker’s mindset” as part of their security team. The unfortunate outcome is that these organizations are likely to suffer greater financial losses.

Having an ERT team in place, and a detailed plan for emergency taking costs into account (and perhaps even cyber-insurance), will help organizations assess their risks and wisely invest in mitigation, thus reducing the business impact of a cyber-attack.

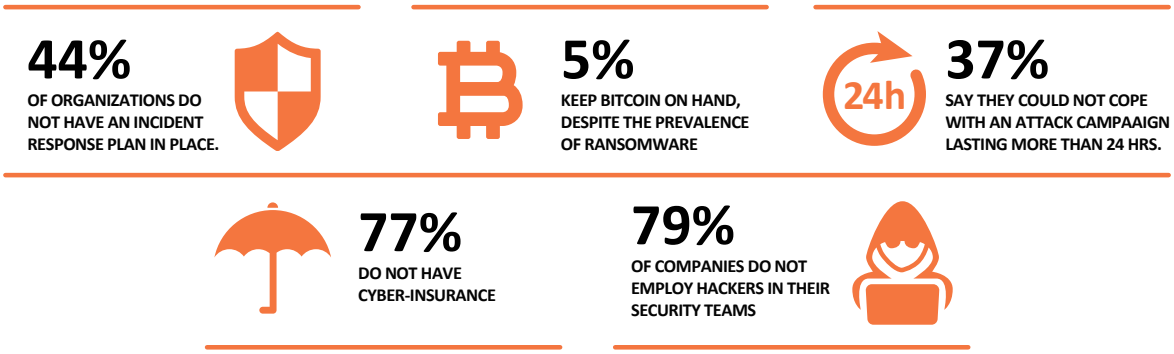


Figure 11: Many European businesses are not fully prepared for today’s threats

Obstacles

With such a diverse threat landscape, it’s no wonder many organizations still admit they may not be prepared to face certain attack vectors. Radware inquired about the cause of this deficiency and discovered one-fourth of security experts said their biggest obstacle was insufficient manpower and a similar percentage (one-fifth) point to inadequate budgets or a lack of expertise.

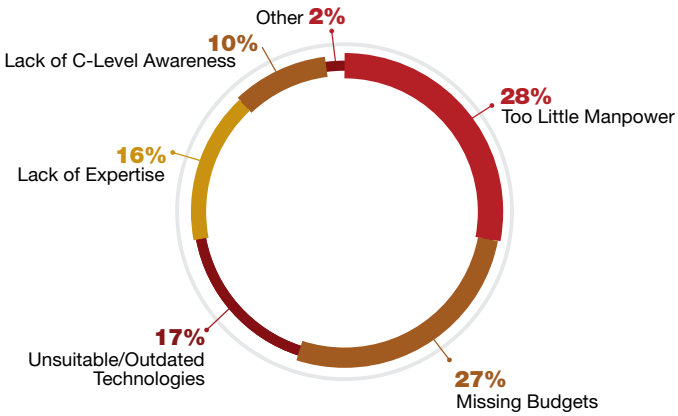


Figure 12: What is your major obstacle when it comes to countering cyber-attacks?

Figures 13, 14 & 15: Preparedness of European organizations compared to other geographies

Of those who do have ERT teams, many prefer to handle situations in-house. Radware is witnessing a growing trend of hiring hackers into security teams, which despite the obvious risk it poses, extends the agility and ability of security teams to identify vulnerabilities and attack forensics.

Actual Costs of Cyber-Attacks

In a world where 98% of organizations are attacked, view cyber-attacks like parasites: not always visible, not always felt, but with plenty of potential to affect your operational efficiencies, service level agreements, and computing resources. All of those impacts bring potentially high costs. Do everything you can to understand the potential impact and build an effective incident response team so you can rein in these "parasites" and limit damage to your business.

Despite the prevalence of cyber-attacks, Radware's 2016 industry survey reveals that the vast majority of Europe's security experts (79%) have not devised a formula for calculating the financial impact of the attacks they suffer. Rather, they rely on estimates. Unfortunately, those estimates tend to be significantly lower than the findings of those who calculate actual costs.

In Europe, only 21% actually came up with a calculation. Sixty-three percent of European businesses believe the loss does not exceed €100,000, and only 12% estimated the cost of an attack to be €1 million or more.

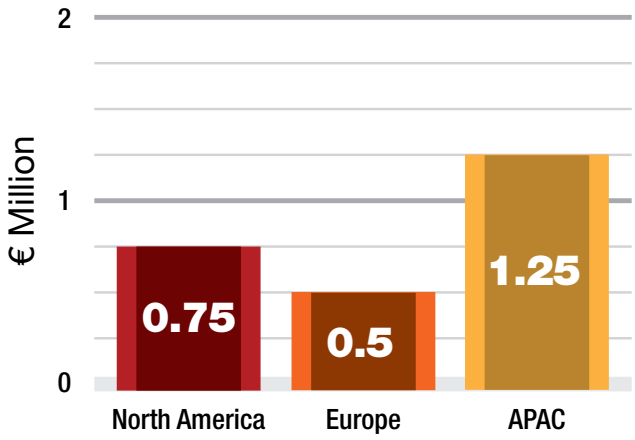


Figure 16: Cyber-attack cost estimation by geography

Planning a Cyber-Combat Strategy

In addition to querying security experts about quantifying cyber-attack costs, Radware also inquired about how organizations currently respond to such incidents. Forty percent of global respondents still lack a formal incident response plan. That's a dangerous shortcoming. After all, cyber-attacks by definition disrupt "business as usual."

How can you plan what to do if you don't know which resources will be available at the moment of attack? Of course, not all attacks are created equal. For many organizations, dealing with a certain threshold of low-level attacks has become commonplace. However, some actually cause serious disruptions that pose a potential threat to the business—and must be handled immediately. How can you tell which is which?

Reducing the Cost

1. **Map Your Risks** - Draw your organization from the inside out, understanding your current information security architecture and looking for vulnerabilities. Consider who might want to hurt you, why, and what means they may have to do so.

2. **Understand the Impact** - Some costs can be easily added to the equation: What is the cost of a minute of downtime? An hour? Are there any legal fees or compliance fines you would face if compromised? What would be the daily cost of investigating an attack?

3. **Prioritize Critical Missions** - Prioritize business procedures and processes, engaging executive management for both their input as well as their endorsement and resource allocation.

4. **Choose Your Squad** - The incident response plan cannot be the sole purview of the cyber security team; other key players in the organization must also know how to orchestrate critical missions when enmeshed in a crisis.

5. **Test, Revise, Adapt** - When a crisis occurs, there is no room for error; your response must be rapid and decisive. To meet that high standard, routinely stage "emergencies" and practice responding to them.

04 WHAT'S ON THE HORIZON?

Four Predictions for 2017

Rise of Permanent Denial of Service

A bot attack designed to completely prevent a victim's technology from functioning, targeting firmware or hardware security flaws. Also known loosely as "phlashing" in some circles, PDoS is an attack that damages a system so badly that it requires replacement or reinstallation of hardware. By exploiting security flaws or misconfigurations, PDoS can destroy the firmware and/or basic functions of system. It is a contrast to its well-known cousin, the DDoS attack, which overloads systems with requests meant to saturate resources through unintended usage.

One method PDoS leverages to accomplish its damage is via remote or physical administration on the management interface of the victim's hardware, such as routers, printers or other networking hardware. In the case of firmware attacks, the attacker may use vulnerabilities to replace a device's basic software with a modified, corrupt or defective firmware image—a process which when done legitimately, is known as phlashing. This "bricks" the device, rendering it unusable for its original purpose until it can be repaired or replaced. Other attacks include overloading the battery or power systems.

Telephony DoS

A cyber-attack targeting communications systems, especially in crisis time. Telephony DoS will rise in sophistication and importance, catching many by surprise. Cutting off communications during crisis periods would impede first responders' situational-awareness, exacerbate suffering and pain, and potentially increase loss of life. A new cyber era could consist of multiple components—including a physical attack with a corresponding cyber-attack targeting the communications systems that first responders use to contain and minimize damage.

Cyber-Ransom Phase 3 – Segmentation

This is expected to evolve and threaten real-time systems such as public transport, medical implants, military devices and more. Imagine if your life depended on an implanted defibrillator or other medical device. Now imagine if such a device were hacked and held for ransom. How about public transportation held hostage? In many ways, cyber ransoming a public transportation system is the ultimate hack—empowering attackers to hold a community hostage for financial or criminal gain. The same applies for automated cars, or aircrafts – as our entire system of transportation is becoming more automated and connected – so it becomes more vulnerable.

Darknet Goes Mainstream

As the value of sensitive data rises in the Darknet marketplaces (for instance – a medical record worth more than a credit card number), with social engineering efforts and recent technologies, we will soon see people's identities traded over the Darknet, unless their online avatars are well secured. Add to that public records, behavioral records, profile briefs and more – somebody can wake up one morning and realize their life now belongs to another.

Tips for a Robust Security Posture

- **Go for Automation** - Continuously adaptive protections are necessary against the ever-evolving application vulnerabilities
- **Prepare for the IoT Tornado** - Use a dedicated DDoS mitigation solution and a scrubbing service before the storm hits you
- **Know Your Enemy** - Knowledge is power -understand hackers' trends, tools and motivations. You can even employ one
- **Reduce Cyber-Attacks' Business Impact** - An emergency response plan or managed services by security experts will restore your operation quickly, protect your data and eliminate associated costs

RADWARE GLOBAL NETWORK AND APPLICATION SECURITY REPORT 05

Key Findings and Stories

Read Radware's 2016-2017 Global Application & Network Security Report to learn more about the following areas:

- **Who attacks you and why** - who the hackers are, their motives and tools.
- **A vertical breakdown** – which verticals are being attacked more frequently, and which attack types they face. It helps readers get a better notion of how they are situated compared to companies like them.
- **Evolution of the IoT botnet** – Extensive research on Mirai code customization.
- **Real life experiences by Radware's customers and partners:**
  - A US carrier CISO walked us through traffic patterns he sees going through his pipes, and highlighted a few DDoS trends.
  - A Leading EMEA Multinational Financial Institution shared with us their experience of being a victim to a DDoS-for-ransom threat by Armada Collective, and also about the impact of an SSL-based DDoS attack on their data center.
  - A US cloud provider contributed their view on protecting sensitive data and how to keep focus when hackers try to steal it from behind a DDoS smokescreen.
  - An India-based Global System Integrator outlines the challenges in securing the distributed application environments today and the imperative need for real-time automation.
- … and a deeper dive into all areas in the European summary

About the Authors

Radware (NASDAQ: RDWR), is a global leader of application delivery and cyber security solutions for virtual, cloud and software defined data centers. Its award-winning solutions portfolio delivers service level assurance for business-critical applications, while maximizing IT efficiency. Radware's solutions empower more than 10,000 enterprise and carrier customers worldwide to adapt to market challenges quickly, maintain business continuity and achieve maximum productivity while keeping costs down.

About the Emergency Response Team (ERT)

Radware's ERT is a group of dedicated security consultants who are available around the clock. As literal "first responders" to cyber-attacks, Radware's ERT members gained extensive experience by successfully dealing with some of the industry's most notable hacking episodes, providing the knowledge and expertise to mitigate the kind of attack a business's security team may never have handled.

For More Information

Please visit www.radware.com for additional expert resources and information and our security center DDoSWarriors.com that provides a comprehensive analysis on DDoS attack tools, trends and threats. Radware encourages you to join our community and follow us on: Facebook, Google+, LinkedIn, Radware Blog, SlideShare, Twitter, YouTube, Radware Connect app for iPhone®.

EUROPEAN APPLICATION & NETWORK SECURITY REPORT 2016-17