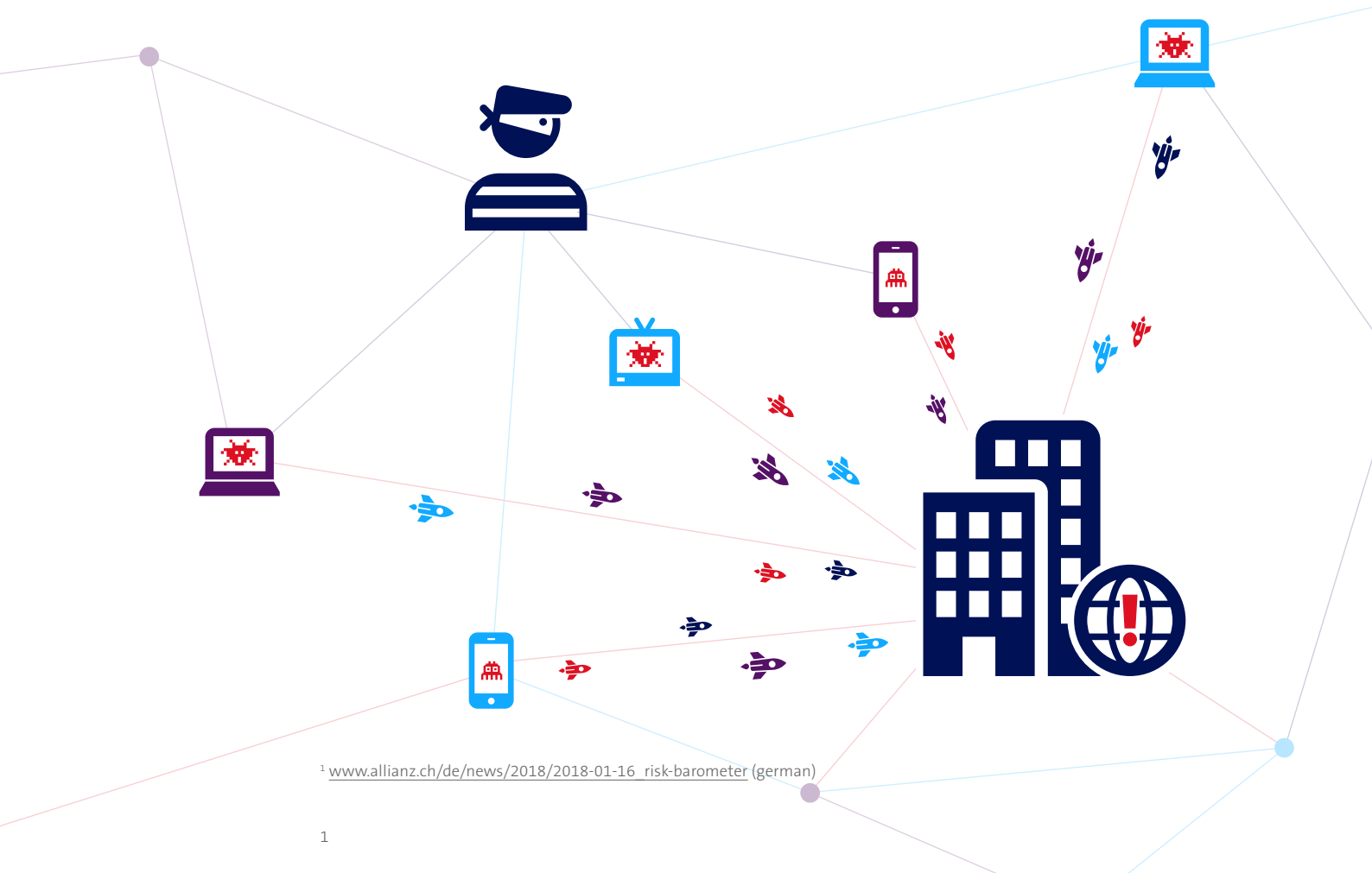
swisscom

SECURITY

Distributed Denial of Service

DDoS Attacks as an IT Security Risk

According to the Allianz Risk Barometer[1], business interruption is by far the greatest risk to business in Switzerland. Cyber attacks rank third in the Allianz Risk Barometer 2018. It should not be forgotten that cyber attacks and business interruption can often be closely linked.



[1] www.allianz.ch/de/news/2018/2018-01-16_risk-barometer (german)

Business risk: inadequate IT security

Cyber attacks and IT disruptions can result in huge financial losses, without damaging or destroying systems or buildings.

The protection of intangible assets, such as data, networks or intellectual property, is therefore becoming an increasingly high priority for risk managers. Inadequate IT security must be seen as a business risk when cyber attacks are capable of paralysing operations. Distributed denial-of-service (DDoS) attacks, in which an IT system or service is simultaneously attacked, overloaded and brought to a standstill by a number of other IT systems, play a key role here.

Overloading and blackmailing via the Internet

If a website, online service or other cloud service is no longer accessible or available, it could be due to a DDoS attack. As indicated in the current management report issued by the Reporting and Analysis Centre for Information Assurance (MELANI)[2], DDoS attacks rank as one of the greatest Internet risks for Swiss organisations. MELANI describes DDoS attacks as "an active tool for attackers with various motivations".

The extent of potential damage caused by a DDoS attack depends on how much the organisation concerned depends on the availability of its online services. As digitisation becomes widespread across all sectors and online services become increasingly important, it must be assumed that DDoS attacks constitute a risk to all industries and may wreak havoc across all sectors.

An organisation may incur financial damage even before a DDoS attack occurs. MELANI reports blackmail attempts on the Internet, where organisations are threatened with a DDoS attack if they refuse to pay the sum of money demanded. In fact, blackmailers do not always have the ability to execute a DDoS attack; they simply hope that the threat alone will be enough for an organisation to pay the ransom.

Nevertheless, it is becoming easier and easier to actually execute DDoS attacks. These days, criminal market places on the Internet offer to execute DDoS attacks as a service, as cyber crime as a service or as a stress test, in return for a minimal fee. DDoS attacks are therefore significantly increasing, as access to these methods of attack has become easy and inexpensive for Internet criminals.

57 %

of organisations sustained an overload of their Internet bandwidth due to DDoS attacks.

[2] www.melani.admin.ch/melani/en/home/dokumentation/reports/situation-reports/semi-annual-report-2-2017.html

The evolution of DDoS attacks and their risks

The potential severity and seriousness of DDoS attacks nowadays is indicated in reports, such as the "NETSCOUT Arbor 13th annual Worldwide Infrastructure Security Report, 2017"[3]:

Threat landscape

- The misuse of IoT devices and the advancement of DDoS attack services are resulting in more frequent and more complex attacks.
- **Scope of threat:** 57 percent of organisations and 45 percent of data centre operators sustained an overload of their Internet bandwidth due to DDoS attacks.
- **Frequency:** According to data from the NETSCOUT Arbor ATLAS Infrastructure (Active Threat Level Analysis System), which covers around one third of global Internet traffic, there were 7.5 million DDoS attacks in 2017.
- **Complexity:** 95 percent of service providers and 48 percent of organisations experienced multi-vector attacks, an increase of 20 percent compared with the previous year. Multi-vector attacks combine large-scale floods, attacks on the application layer and TCP state-exhaustion attacks in a single, persistent offensive, which increases the complexity of defence (mitigation) and the attacker's chances of success.

Consequences

- Successful DDoS attacks have greater operational and financial consequences.
- 57 percent cited one consequence as being the damage caused to reputation/brand, followed by operating costs.
- 56 percent suffered financial consequences ranging from 10'000 to 100'000 dollars, almost twice the figure for 2016.
- 48 percent of data centre operators cited customer migration following a successful attack as a key problem.

Defence

- Network and security teams face challenges as a result of an active and complex threat landscape as well as ongoing personnel issues.
- 88 percent of service providers use intelligent DDoS mitigation solutions and 36 percent use technologies that automate DDoS mitigation.
- The frequency of attacks also increases the demand for managed security services. 38 percent of organisations rely on third party and outsourced service providers, an increase of 28 percent compared with the previous year. Only 50 percent conducted drills and the proportion of respondents undertaking quarterly drills fell by 20 percent.
- 45 percent of organisations and 48 percent of service providers find it difficult to recruit and retain qualified security personnel.

Current DDoS attacks

For anyone needing visual evidence of the current scope of DDoS attacks, providers, such as NETSCOUT Arbor and Akamai, maintain an up-to-date overview of the DDoS attack situation:

Digital Attack Map (top daily DDoS attacks worldwide) provided by NETSCOUT Arbor: www.digitalattackmap.com

Real-time Web monitor provided by Akamai: www.akamai.com/uk/en/solutions/intelligent-platform/visualizing-akamai/real-time-web-monitor.jsp

[3] https://www.netscout.com/report

DDoS attacks in Switzerland

DDoS attacks occur daily, round-the-clock, and have a tangible effect on Swiss organisations, as reported regularly in the media. The number of DDoS attacks seen on Swiss organisations continues to increase.

For example, the NETSCOUT Arbor Active Threat Level Analysis System (ATLAS) indicates that, in May 2018, an average of 227 DDoS attacks per day were committed on Swiss organisations. The largest DDoS attack in Switzerland in May 2018 had a magnitude of 10.7 Gbps. One of the largest attacks previously seen in Switzerland involved a volume of 55 Gbps on a single organisation.

The following sample headlines from **Switzerland's daily newspapers** show how serious these attacks can be:

- Criminals blackmail Swiss online shops (NZZ am Sonntag, March 2016)[4]
- "Grey Hats" attack SBB website and hack SVP database (Tageswoche, March 2016)[5]
- A new wave of blackmail: Swiss online shops threaten a Black Friday (Badener Tagblatt, April 2016)[6]
- Extreme right-wing hacker attacks left-wing websites (Aargauer Zeitung, February 2017)[7]

The **Federal Office of Police (fedpol)** reported blackmailing attempts executed by means of DDoS (Distributed Denial of Service). For example, one group behind the DDoS attacks was Lizard Squad:

- Victims received an e-mail written in English. The sender was lizardlands@lizardsquad.net. In the e-mail, victims were demanded to pay 10 bitcoins (approx. CHF 6280) by a certain date. The blackmailers threatened to launch a DDoS attack on the victim's information system if they failed to comply with the demand.

[4] https://www.nzz.ch/nzzas/nzz-am-sonntag/cyber-attacken-kriminelle-erpressen-schweizer-online-shops-ld.9083

[5] https://tageswoche.ch/allgemein/grey-hats-greifen-sbb-website-an-und-hacken-svp-datenbank

[6] https://www.badenertagblatt.ch/wirtschaft/neue-erpresserwelle-schweizer-online-shops-droht-ein-schwarzer-freitag-130227864

[7] https://www.aargauerzeitung.ch/schweiz/rechtsradikaler-hacker-attackiert-linke-websites-130956850

(all sources german)

The **Reporting and Analysis Centre for Information Assurance (MELANI)** reported a number of such attacks and the associated blackmail perpetrated by the groups known as the Armada Collective and DD4BC, which have caused something of a media sensation in Switzerland. MELANI strongly advises against complying with the demands of these blackmailing groups:

- Faced with the pressure of a threat to their website and in the hopes of a "quick" solution, some organisations do consider making a payment to the blackmailers. By making such a payment, not only do these organisations allow the perpetrators to succeed, they also give them the financial means to strengthen their attacking infrastructure and intensify their attacks.
- Attackers often use what are known as booter or stresser services, as detailed by MELANI. These are tools that initiate DDoS attacks in exchange for payment ("DDoS as a service"). The more money an attacker has at their disposal, the greater the attack volumes (in terms of both intensity and length) they can purchase from one of these criminal service providers. In contrast, if no ransom is paid, the criminal's business model fails. MELANI therefore discourages the payment of any ransom.

The **Federal Intelligence Service (FIS)** refers to DDoS attacks in connection with the Internet of Things (IoT) in the current management report 2018 (Security for Switzerland)[8]:

- Attackers take advantage of the IoT by misappropriating the availability of insufficiently protected devices, such as web cams, baby phones or smart TV systems for attacks. This is particularly worthy of note since the attack on the Internet service provider Dyn, perpetrated by the Mirai botnet, which infects devices in the Internet of Things. Mirai is a malware that attacks LINUX operating systems used primarily in devices for the Internet of Things.

DDoS attacks have also been the subject of an inquiry within the **Federal Assembly,** as the federal government supports cantons in the prosecution of DDoS attacks where there is a lack of expertise.[9]

227

attacks were committed on average per day on Swiss organisations in May 2018.

[8] https://www.admin.ch/gov/en/start/documentation/media-releases.msg-id-70611.html

[9] https://www.parlament.ch/en/ratsbetrieb/amtliches-bulletin/amtliches-bulletin-die-verhandlungen?SubjectId=38493

DDoS attacks: easier, yet more complex

A number of developments in the field of cyber crime are ensuring that the already huge risks inherent in DDoS attacks become even greater:

- DDoS attacks are becoming easier; they can be purchased in criminal online marketplaces and paid for with stolen credit card details. Their execution requires no IT expertise; for a small fee, any criminal can commission criminal DDoS service providers to execute the relevant attacks.
- DDoS attacks are targeted. They are not initiated at random, but rather pursue a precise objective, such as to paralyse a company's website. The party commissioning the attack may be, for example, one of the victim's competitors.
- Whilst the consequences of a DDoS attack may become apparent immediately, because, for example, the website of the company concerned can no longer be accessed, the sources and party commissioning the DDoS attacks are not so easy to identify and thus not so easy to intercept.

Consequently, DDoS attacks are easy to perform, but complex to ward off.

Why and how DDoS attacks are executed

DDoS attacks are executed for various reasons, as MELANI explains. The motivation behind DDoS attacks is usually political activism, blackmail or to damage the finances or reputation of a competitor:

- If a website is inaccessible, this can result in a huge loss of profit or reputation for the owner, particularly if the service being attacked is of a commercial nature.
- In many cases, a DDoS attack is accompanied by a demand for money. The blackmailer demands money to stop an attack they have already initiated or to refrain from initiating an attack. The attackers hope that the victim will pay, so as not to suffer any negative consequences of such an attack.
- A DDoS attack can also be used to divert traffic from a data theft running in parallel or as a means of system hacking.

The range of motives makes it clear that any company or organisation can fall victim to DDoS attacks.

Europol case study

In close cooperation with fedpol, the European Union Agency for Law Enforcement Cooperation, known as Europol, has recently reported on a DDoS marketplace. The Europol report illustrates how these marketplaces work and highlights the huge risk resulting from the easy, inexpensive access criminals have to DDoS attacks, requiring no IT expertise:

- The administrators of the DDoS marketplace webstresser.org were apprehended on 24 April 2018 as a result of Operation Power Off, a complex investigation conducted by the Dutch police and the British National Crime Agency with support from Europol and a dozen or so law enforcement authorities. The illegal service was brought to a standstill and its infrastructure sequestrated.
- Up until April 2018, webstresser.org was one of the world's largest marketplaces for DDoS services, with more than 136'000 registered users and 4 million attacks. The orchestrated attacks affected critical online services of banks, government institutions, the police and the gaming industry.
- Initiating a DDoS attack like this would once have required a fairly good knowledge of Internet technology. That is no longer the case. With webstresser.org, the fees for commissioning DDoS attacks only amounted to 15 euros per month, enabling people with even the most limited financial resources and lack of technical skill to initiate harmful DDoS attacks.

Europol concludes that[10]:
Criminals use DDoS attacks as a means of attacking both private companies and the public sector. Attacks like these are not only for financial gain; they are also used for ideological, political or purely malicious reasons. Not only is this type of attack one of the most frequent, it is also more easily accessible and costs little in terms of finance and risk to the attacker or commissioning party.

15 Euro
per month were the fees at webstresser.org for commissioning DDoS Attacks.

[10] https://www.europol.europa.eu/internet-organised-crime-threat-assessment-2018

The consequences of DDoS attacks

To be able to analyse the risks and take preventative measures that are appropriate to the threat, it is important to gain an overview of the potential consequences: organisations that fall victim to a successful DDoS attack suffer multiple forms of damage, as regards both the IT systems affected and the organisation as a whole.

Damage to IT systems

Systems attacked	Servers, networks, operating systems and applications are overloaded and brought to a standstill.	Data transmissions are brought to a standstill, online services and connected internal systems are slowed down or break down completely.
To attack misused systems	Servers, terminals and IoT devices are infected with malware (bot) and become part of a botnet. As well as computers, networked equipment, such as Internet-capable televisions, surveillance cameras, routers, or set-top boxes can be misused for botnets and DDoS attacks. Security experts point out that, depending on the type of attack and organisation under attack, a few dozen of misused devices (bots) may be all that is required to successfully execute a DDoS attack.	The attackers (bot masters) control systems remotely, with users often not being aware that their system is part of a botnet.

Damage to the organisation as a whole

Loss of sales	Websites and other online services are no longer available for customers and partners. Orders, entries and other transactions cannot be completed.
Damage to reputation	Customers and partners become upset and often switch to a competitor.
Loss of data	Data is lost, manipulated or deleted.
Higher costs, falling productivity	Expenses in the IT department, support, customer service and legal department increase significantly as a result of upset customers and partners, calls to the hotline and potential claims for the non-fulfilment of contracts. At the same time, productivity falls as the company's employees can no longer undertake online activities.

The diversity of DDoS attacks

It is important to understand the various types of DDoS attack to gain a better understanding of the risks and how to develop a defence strategy.

The various types of DDoS attacks

DoS vs. DDoS vs. DRDoS attacks

"Denial-of-service" **(DoS)** attacks result in hugely restricting the availability of certain online systems and/or services or fully denying access to these.

With "distributed denial-of-service" **(DDoS)** attacks, the attacker makes use of the service of a number of misused systems (a botnet). The number of systems involved in an attack (PCs, smartphones, IoT devices) can vary from a few hundred to several hundreds of thousands of systems attacking simultaneously. Even the most powerful of online systems can therefore be successfully disrupted with broadband network connections.

With a "distributed reflected denial of service" **(DRDoS)** attack, the attack is made indirectly. The attacker sends their data packet to Internet services, rather than directly to the victim. However, they register the victim's IP address as the sender's address. This method makes the origin of the attack practically impossible to identify ("IP spoofing"). The response of the data packets by the Internet service and the resulting system overload for the actual victim constitute the indirect DoS attack.

Volume-based attacks

With **volume-based attacks,** attackers flood a website with traffic to completely consume the website's available bandwidth. As a result, legitimate data traffic cannot get through and the website is no longer accessible for legitimate users.

With volume-based attacks, a botnet can send several Gbps within seconds and overload the connection or firewall.

Application layer attacks

Application layer attacks target security loopholes in applications such as Apache, Windows and OpenBSD. Application layer attacks bring servers to a standstill by launching a huge number of requests to an application, which at first appear to be legitimate, by imitating a user's usage behaviour.

Protocol attacks (such as SYN flooding, ICMP flooding, HTTP flooding)

Protocol attacks aim to fully consume server resource capacity.

With **SYN flooding,** the attacker sends a data packet to set up a connection to the victim's system. This reserves a port and returns a packet. However, as the attacker does not use their own IP address, the sender does not receive any confirmation. The victim's system repeats and finally rejects the reserved connection after a set period of time, which can amount to several minutes, depending on the operating system. If this connection is then set up repeatedly for multiple parallel executions, this results in the computer being practically blocked by being overloaded with responding to requests.

With **ICMP flooding or ping flooding,** the victim's system is overwhelmed with ICMP "echo request" (ping) packets. This type of attack can consume both outgoing and incoming bandwidth, as the victim's systems attempt to respond with ICMP "echo reply" packets, which results in considerably slowing down the entire system.

With **HTTP floods,** the attacker uses what appear to be legitimate HTTP GET or POST requests to overload a web server or application.

DNS attacks

With a **DNS flood,** the attacker aims for a particular area on one or more DNS servers (domain name system) and attempts to disrupt DNS resolution of resource entries in this area and its subareas by overloading the DNS servers.

With **DNS amplification,** the attacker exploits security loopholes in DNS servers to convert what are initially small requests into much larger loads that are used to cause the victim's servers to crash.

100–100'000

running devices (PCs, smartphones, IoT devices) can simultaneously be misused as attacking systems.

Resisting and mitigating DDOS attacks

Various procedures are used and offered for the resistance and mitigation of DDoS attacks. Clearly the most effective control of unwanted data traffic ideally takes place in an Internet Service Provider's (ISP) backbone and not just at the actual endpoint, which can be overloaded by attacks.

Procedure for resisting and mitigating DDOS attacks

Black hole

Unwanted data traffic is routed to a black hole (on the router ports of the backbone transfer) and rendered harmless.

Note: Blackhole technology only provides the web infrastructure with limited protection against attacks.

All data traffic is deleted, meaning that the organisation can no longer receive data from certain network segments and regions, not even legitimate data traffic that the organisation would like to receive.

Active DDoS filtering (anomaly recognition)

Data traffic is constantly monitored (in the backbone). If a deviation from the baseline (= bandwidth flow registered continuously over a 24-hour period) occurs, depending on the deviation, an alarm is issued proactively and/or automatic filtering is commenced. The organisation can use the alarm information to specifically address or combat the DDoS attack.

Note: Anomaly assessment requires in-depth expertise. If this expertise is lacking, a service provider with a high-performing backbone with protection against DDoS attacks should be evaluated.

Malicious traffic rerouting/ legitimate traffic forwarding

A solution for threat intelligence/security intelligence analyses data traffic and can distinguish between harmless and harmful traffic and filter it accordingly. Filtered, and hence authorised, traffic is then forwarded to the original destination; harmful traffic is diverted and rejected.

Note: Activating this type of filter function should be initiated by the actual organisation, even if a service provider is used. A sound knowledge of the organisation's network operation avoids false alarms which would otherwise be triggered, for example, by a scheduled software upgrade.

Conclusion

When evaluating business risks, the digitisation of our economy and society means that cyber risks are becoming increasingly significant. Cyber attacks, such as DDoS attacks, rank as some of the most significant and dangerous causes of operational interruption.

Numerous incidents in Switzerland show the reality of the risks resulting from DDoS attacks for Swiss organisations. The Swiss security authorities are on alert and provide detailed reports of DDoS attacks and the measures required to counter them. The potential damage to Swiss organisations ranges from loss of data, loss of sales, and damage to reputation to breaches of contract, as services promised to customers cannot be provided if the necessary online services fail.

These days, it is very easy to execute DDoS attacks. Attackers do not have to be hackers themselves. They can employ criminal services, enabling them to wreak major havoc with minimal effort. Attackers' motivation is complex. The targets of attacks are well defined; vulnerabilities and bottlenecks in Internet bandwidths, applications and communication protocols are exploited. Identifying and mitigating these attacks is therefore becoming increasingly complex; the need for action regarding DDoS protection is urgent.

The Reporting and Analysis Centre for Information Assurance, MELANI, stresses that DDoS can affect any organisation and can have far-reaching economic consequences for victims. Organisations must therefore take measures to protect themselves against potential DDoS attacks.

If an organisation is threatened with a DDoS attack and requested to pay a ransom, MELANI recommends making suitable technical arrangements with the host/provider to prepare for a possible attack. However, even if the organisation is not actually threatened, but online services are essential for business operation, preventative protective measures are given.

The progressive digitisation of Swiss organisations means that this recommendation from MELANI is relevant for every organisation: protective measures against potential DDoS attacks should not just be taken with the threat or occurrence of an attack. The saying that "prevention is better than cure" applies just as much in this context as any other. Without DDOS protection being proactively managed, an organisation's online presence and Internet usage is rendered impossible.

Act now!

Protect your networks and infrastructure effectively against DDoS attacks.
Please take our advice!

Do you have any questions? Please contact
Cyrill Peter and the Security Product Management Team
productmanagement.security@swisscom.com

Further information about DDoS is available at www.swisscom.ch/ddos

Further information about cyber security is available at www.swisscom.ch/security