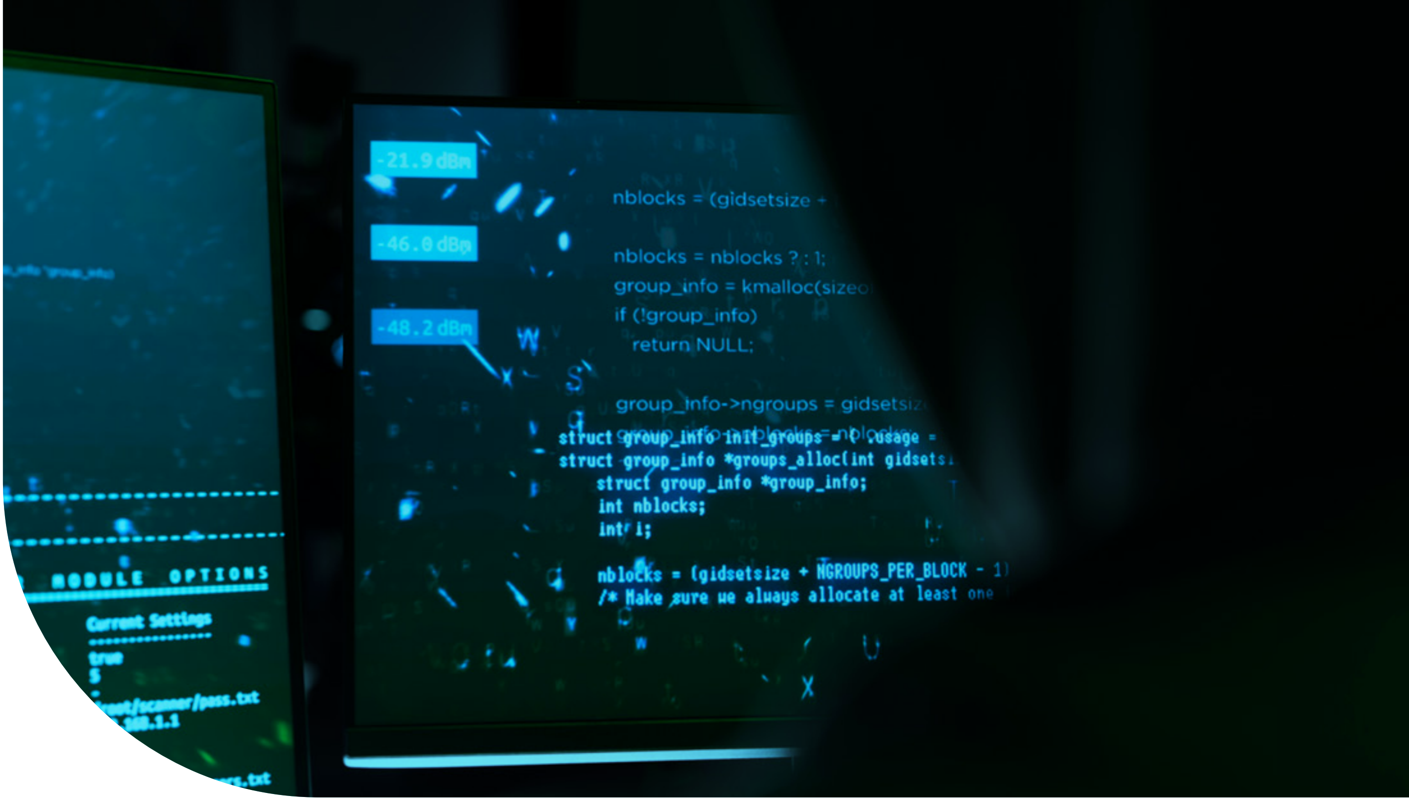
IT CONTINGENCY PLAN

How to prepare for a cyberattack

Digital Security
Progress. Protected.



```
nblocks = (gidsetsize +

nblocks = nblocks ? : 1;
group_info = kmalloc(sizeo
if (!group_info)
  return NULL;

group_info->ngroups = gidsetsiz
struct group_info init_groups = { .usage =
struct group_info *groups_alloc(int gidsets
    struct group_info *group_info;
    int nblocks;
    int i;

    nblocks = (gidsetsize + NGROUPS_PER_BLOCK - 1)
    /* Make sure we always allocate at least one
```

Suddenly, all the computers go into sleep mode, the website is down, and none of your employees can access the network or the data. The whole IT suddenly comes to a standstill. As it turns out, things stay this way for the next four weeks because the company isn't prepared for this type of incident. Many organizations, especially the small and medium-sized ones, aren't prepared for this kind of crisis, caused by cybercriminals. What should you do if you encounter a cyberattack?

Although cyberattacks have been on the rise during the past years, and the COVID-19 pandemic even accelerated the trend, the topic is still underestimated in many companies. According to the 2021 CNBC | Momentive Q3 Small Business Survey, 56% of America's small business owners said they were not concerned about being the victim of a hack in the next 12 months, and 24% said they were "not concerned at all."

What is more, only 28% of small businesses said that, in the event of a cyberattack, they have a plan in place for response, 42% said they have no plan, and 11% revealed they were "not sure" if their businesses had plans in place.

13%

Proportion of smaller businesses that train staff on cybersecurity. Only 19% have tested their staff responses, for example, with mock phishing exercises.

Source: Ipsos MORI and UK Government Department for Digital, Culture, Media and Sport survey, 2021

Experts rate this behavior as negligent. It's no longer a question of if, but when cyberattacks will happen. This was confirmed by a survey published in 2021 by the German digital association Bitkom.

9 out of 10

Almost 90% of 1,000 companies from all sectors surveyed in Germany reported being affected by cyberattacks. Which types of attacks were mentioned the most among them?

Malware

Phishing

XSS

Attacks on passwords

Ransomware

DDoS

Man in the middle attack

SQL injection

Spoofing

86%

of companies experienced damage caused by a cyberattack. In 2019, this figure was only 70%.

Source: Bitkom Research, Germany, comparison of surveys from 2019 and 2021

Getting started with an effective contingency plan

Experts in acute and emergency medicine call the decisive phase in life-threatening injuries or illnesses the "golden hour." The faster the response, the better the chances of a complete recovery. Professional business continuity management is a prerequisite for a successful golden hour in an operational context. **The goal is to increase the reliability of processes and respond rapidly and systematically in an emergency** – and especially in the event of hacker and malware attacks.

The contingency plan, also known as IT incident management. Typically encompasses the entire organizational and technical process for responding to detected or suspected security incidents or malfunctions in IT areas, as well as preparatory measures and processes. The spectrum of possible incidents ranges from technical problems and weak points to specific attacks on the IT infrastructure. IT incident management in the narrower sense must **take into account all organizational, legal, and technical details**.

The chances of hackers completing a successful attack are manifold and extremely high. The cybercriminals themselves are now highly professional. Today's hackers have at their disposal various profitable means of manipulation and ways of spreading blackmail trojans, viruses, etc., in the network. And **a cyberattack is not always immediately noticed**, because not all system levels are under observation.

Good preparation is crucial when it comes to the creation of a contingency plan. This is because, should it come to the worst-case scenario, the most important thing to do is **respond quickly**, stopping the attack as quickly as possible, protecting the stored data, and also restoring the company's normal operations as soon as possible.
A variety of immediate measures, therefore, need to be defined: for example, when the entire office communication network collapses,

websites are no longer available, or even the entire production process comes to a standstill after an attack.

What to do when drawing up a contingency plan

- **Develop an operational contingency plan:** Record all necessary measures that must be taken in the event of an emergency. It is best to seek professional advice from experts. An initial overview can also be found in sample templates.
- **Designate an IT security officer:** Designate a responsible person to deal with security issues in the company. Since the GDPR was introduced, businesses with more than 10 employees must appoint a data protection officer.
- **Check your current contingency plan:** If you already have a contingency plan, you should have it checked and implemented by experts. You should also make sure that your contingency plan is comprehensible to laypeople.
- **Prepare your company for all eventualities:** In order to really know whether the plan works, you must test it in practice in advance.

Cyberattack: What to do in a crisis

As time passes, cybercriminals are causing more and more damage, infiltrating the IT architecture down to the smallest element, or syphoning off extremely sensitive data. IT managers are therefore tasked with recognizing harmful activity at an early stage, and acting quickly. This is the only way to minimize the damage caused, and even to avoid the total failure of the system as a whole. In addition to the financial consequences, companies must, above all, fear a huge loss of image and trust on the part of customers. So, what should companies do when criminals have hijacked corporate data and office communications are out of order?

Where to turn in case of a cyberattack

- IT retailers and system vendors have a wealth of experience with cyberattacks and can give fast, targeted assistance.

- If possible in your country, the incident should be reported. For example, if you're from the United Kingdom, you can report it online to Action Fraud, and in the US, you can file a complaint on the FBI website.

9 tips that help you reduce the impact of a cyberattack to a minimum

1. Keep calm and act tactically

If IT security software sounds the alarm, the first thing to do is keep calm. A successful cyberattack often comes as a surprise. For example, a malware can sometimes hide in the network for weeks without being noticed if IT fails to monitor all system levels. But when an incident occurs, it is important to make the correct decisions in the shortest possible time. Without a contingency plan with defined immediate measures, chaos can be effectively pre-programmed.

2. Determine the extent of the infection

Many IT departments of companies that are victims of malware attacks rely on their intuition rather than in-depth analysis to determine the consequences of such attacks. Of course, it is important to respond – but not on the basis of assumptions. If a company has a functioning IT emergency management plan the IT department can quickly find the right answers to central questions:

☑ Which systems have been infected?

☑ How did it happen?

☑ Have business-critical data been lost?

☑ Is the infection only affecting individual components, or an entire subnetwork?

☑ Has customer information and employee data fallen into the hands of the attackers?

3. Ensure IT operations

If internal information has fallen into the hands of unauthorized persons, the affected employees and customers must first be informed. If IT systems have been severely affected by an attack, backup systems and redundant network connections should be activated, because the business must not suffer from a cyberattack. In order to ensure this, a contingency plan is also required in order to shorten the response times.

4. Contain the infection

The infected IT systems must then be isolated. In order to prevent the spread of the infection in the network, the IT department can disconnect the network segments in which the infected computers are located. This means that attackers no longer have access to these systems, and cannot "syphon off" usable data.

In any case, the IT department should try to decode the encrypted data traffic between the infected IT systems within its own network and the attackers' computers. This allows them to determine whether other computers in the network have been contaminated, and which firewall rules are required to prevent unauthorized access. These countermeasures can be implemented much faster and more efficiently if a company is using an IT security solution — for example, ESET's new business solutions.

5. Secure evidence

Evidence of incidents must be kept to allow law enforcement authorities to take action after a successful attack. Comprehensive documentation may also help you to claim on an existing cyber insurance policy.

6. Eliminate the infection and prevent further attacks

One of the most demanding tasks is to clean the affected IT systems of malware and put a stop to further attacks in the same way. One proven tool is antivirus or anti-malware software that automatically cleans IT systems. In order to prevent further attacks of the same kind, the security loopholes that made these activities possible should be eliminated. To be absolutely sure, it is advisable to analyze data packets that are transported over the network. Traffic should be investigated, in particular, for traffic patterns and commands previously used by the attackers.

Other security precautions include checking the firewall rules and changing the passwords that employees use to log on to the network. A deeper analysis of the cyberattack is worth considering, because, in many cases, individual attacks are part of advanced persistent threats (APT). These are continuous, complex, and targeted cyberattacks on SMBs or their employees. If management becomes the target of such APTs, it can be assumed that further attacks will follow.

7. Legislation – GDPR and other relevant regulations

Legal issues arise after a cyberattack – these should be clarified in advance. Since the introduction of the GDPR, certain incidents must be reported to authorities within a certain period of time. Information obligations should be clarified in advance with your legal department, so that your company remains legally compliant and does not have to pay any additional fines afterward.

8. Don’t pay when ransomware attacks happen

Blackmail software is a popular means of attack by cybercriminals. The malware encrypts the victims’ data and the hackers then demand a ransom to release it. Never pay the ransom demanded – because you can’t be sure that you’ll get your data back. In addition, you are supporting this financing model of cybercriminals and signaling your willingness to pay, which hackers take as a new invitation.

9. Learning from cyberattacks and mistakes

It is important that companies draw the right conclusions from the analysis of attacks, and take appropriate precautions. Any previously unknown vulnerability that has been remedied ultimately presents an opportunity to improve defensive measures at the perimeter of the corporate network and close potential entry points. It is also crucial that the IT manager keeps a close eye on all system levels. This facilitates the detection of a cyberattack at an early stage, and doesn’t give intruders the opportunity to immerse themselves in specific areas and scout the system before they start the attack itself.

In case of a cyberattack, make sure that:

- No further damage can result from the attack.
- Immediate measures can be taken independently of higher-ranking departments or the executive level so that no time is lost obtaining approval in the event of a crisis.
- Login data can be changed immediately. Stolen passwords, logins and contaminated email accounts can cause further damage in the future. Your contingency plan should therefore include a strategy for how to proceed after a hacker attacks with company-owned access data.
- Even guest accesses, if they exist, are deactivated and the network goes offline. Unmanaged guest devices in particular pose a high risk for malicious code entering the system.
- No emails are opened, mobile devices are not logged into the company network or other networks, e.g. customer networks, and all storage media connected to the network, such as USB sticks, external hard drives, cameras, etc., are disconnected and neither used nor removed from the workplace.

5 extra tips for greater security

If you take the steps listed above, you are already very well prepared for a crisis. Here are five more recommendations that will help you to optimize security in your company:

1. Automate as much as possible

In the best-case scenario, the emergency plan can be largely automated and use modern tools. All processes that can be executed autonomously relieve the burden on the administrator. These actions can include, for example, the automatic encapsulation of affected endpoints, where the desktop firewalls cut off all connections except those of remote administration.

2. Pay attention to logging and documentation

It is also important that all actions, whether automatic or manual, include the comprehensive logging and documentation of manual steps. This is the only way to track the infection process retrospectively and adapt the contingency plan accordingly – as far as the closing of possible security gaps, but also human behavior, is concerned.

3. Make regular backups

Whatever has caused the security incident, the ability of companies to recover lost, business-critical data as quickly as possible is crucial. This starts with regular backups. Here, too, the automatic backup of data copies is a good choice, because this ensures the consistency of information. In addition, you ensure that employees do not forget to make backups. Backup copies should be made on at least two external media, and an encrypted version of a backup in the cloud storage should also be considered (with respect to data protection, you should rely on European storage locations). Again, backup and recovery systems must be tested regularly.

4. Use an endpoint detection & response (EDR) tool

An EDR tool allows the constant and comprehensive monitoring of all endpoint activities. Suspicious processes can then be analyzed in detail, and IT managers can respond to threats at an early stage. Companies enhance their security measures many times over with the use of EDR technology, especially in the event of zero-day attacks, ransomware, targeted attacks (advanced persistent threats), or violations of internal company policies.

5. Regularly review your contingency plan

Just like fire drills, IT contingency plans must be tested regularly. Nothing is more fatal than to rely on a plan that ultimately doesn't work.

Conclusion

The contamination of PCs, servers, or mobile systems with malicious software can pose a serious threat to organizations – especially when internal information falls into the hands of attackers. However, such incidents bring two important facts to the attention of those in charge: on the one hand, which IT security measures need to be optimized, and on the other, the fact that an up-to-date contingency system can minimize damage.

Digital Security
Progress. Protected.

When technology enables progress, ESET is here to protect it

For more than 30 years, ESET® has been developing industry-leading IT security software and services to protect businesses, critical infrastructure and consumers worldwide from increasingly sophisticated digital threats. From endpoint and mobile security to endpoint detection and response, as well as encryption and multifactor authentication, ESET's high-performing, easy-to-use solutions unobtrusively protect and monitor 24/7, updating defenses in real time to keep users safe and businesses running without interruption. Evolving threats require an evolving IT security company that enables the safe use of technology. This is backed by ESET's R&D centers worldwide, working in support of our shared future. For more information, visit eset.com or follow us on LinkedIn, **Facebook**, and **Twitter**.

Home

Businesses

Governments

110 000 000+
Protected users worldwide

300 000+
Unique new malware samples detected daily

600+
Research and development experts

400 000+
Business customers in 200+ countries and territories

© 1992–2022 ESET, spol. s r.o. – All rights reserved. Trademarks used herein are trademarks or registered trademarks of ESET, spol. s r.o. or ESET North America. All other names and brands are registered trademarks of their respective companies.