Alinto

White paper

November 2021

Business email communication : how to protect your company from cyber attacks?

Summary

Tighten the net

Only one in two companies report being equipped and prepared to deal with a cyber attack1. This is a sad fact that leads organisations to rethink the security of their IT network, and more particularly their professional email.

Indeed, the majority of cyber-attacks come from fraudulent emails. And the techniques and technologies used by hackers are becoming increasingly sophisticated. They are now targeting all companies: from small businesses to multinationals, taking advantage of the low awareness of employees regarding malicious emails.

The most diligent companies implement strict security systems: firewalls, patching, anti-spam, etc. Nevertheless, these protections, often linked to the network, system and messaging solutions in place, have their limits. An email can slip through the nets.

In this White Paper, we take a look at cyber-attacks, review best practices for strengthening email security, and offer our advice on how to better protect your organisation.

[1] 6th edition of the CESIN annual barometer

Email security: state of the art

It cannot be stressed enough that email is the preferred channel for cyber-attacks. And this is increasing year after year, despite improvements in the security of personal and professional email, user awareness and the dissemination of and the distribution of alerts about phishing and cyber-attacks. For their part, cybercriminals are using increasingly sophisticated malware and their techniques are more sophisticated and can therefore be confusing.

Ransomware, phishing, malware... are all threats for companies, which must therefore be particularly cautious and make their employees aware of these threats. All the more as cybercriminals are surfing on the Coronavirus pandemic using fear to encourage people to click.

To see the situation more clearly, we offer you an overview of the situation.

Cybersecurity: the worrying increase in email attacks

By 2020, cyber-attacks have quadrupled compared to previous years[1] . Cybercriminals are now better organised, send numerous fraudulent emails and target vulnerabilities in companies' IT networks. Attacks are industrialised, planned. We are far from a person acting alone behind his computer.

Here are some statistics to illustrate the current situation and the vulnerability related to messaging in France:

- Ransomware accounts for 11% of the total volume of malicious emails[2].

- 80% of French companies cyber-attacked in 2020 were attacked via phishing emails or spear-phishing[3].

- In 2020, one out of five companies declare having suffered at least one ransomware attack during the year[4].

- Only one in two companies is confident in its ability to deal with a cyber-attack[5] .

- The health crisis brings new risks: 35% increase in cyber attacks[6].

- 57% of companies plan to increase their cybersecurity budget[7].
- 85% of companies plan to acquire new technical solutions to improve their IT security[8].
- 75% of emails received are unwanted[9].
- Reports to the government of cyber attacks from professionals have increased by 30% compared to 2019[10]

The development of teleworking, the fear induced by the pandemic, the development of the cloud, the professionalisation of email attacks explain this evolution. There is no sign of a change in trend: the phenomenon is likely to continue for years to come and remain a real concern for organisations.

Cyber attacks: significant impact for businesses

It is difficult to estimate the cost of a cyber-attack. This is not only reflected in the economic consequences, but also in the impact on the company's reputation, the fragilization of the IT infrastructure, or the operational difficulties.

In 2020, 58% of cyber attacks had a proven impact on business, with direct disruption to production in 27% of cases[11] .

The main consequences of the attacks[12] can be broken down as follows:

- Data theft (30%)
- Denial of service (29%)
- Business interruption due to data encryption by ransomware (24%)
- Identity theft (23%)

A study by Bessé shows that the risk of a company's failure increases by 50% in the three months following the announcement of a cyber-attack. This risk can even reach 80%[13] .

Another study by the IBM Ponemon Institute found that 80% of French companies do not have an incident management plan. Another significant finding is that it takes an average of 201 days for a company to discover that it has been the victim of a cyber-attack. The direct consequences can also hit customers if their personal data has been compromised.

A simple click on a link in an email can therefore irremediably weaken the entire company. This is why it is important to continue to raise awareness among employees, but also to strengthen IT security through various dedicated email protection solutions.

[1] Cyber-attacks quadrupled last year, says cybersecurity expert - France TV info
[2] Intervention Devensys - Methods to improve your email security 2018
[3] The most common cyber-attacks against French companies - Statista
[4 to 8] 6th edition of the CESIN annual barometer
[9] Messaging: numbers and threats - security dsisionnel
[10] Cybersecurity: more reports in 2020 - vie-publique magazine
[11] 6th edition of the CESIN annual barometer
[12] The most common cyber-attacks against companies, CESIN and OpinionWay
[13] On a panel of SMEs

Some examples of cyber-attacks and their impacts :

- A hospital in New Jersey (USA) paid a ransom of over $600,000 (2020).
- Verne Harnish, CEO of Gazelles Inc. was robbed of $400,000 from his bank account when hackers gained access to his computer and intercepted emails between him and his assistant (2019).
- EasyJet has announced that it has been the victim of a major cyber-attack: more than 9 million customer data (email addresses and travel information), including 2,000 credit card details were illegally accessed (2020).
- The University of California at San Francisco (UCSF) was hit by a ransomware attack that paralysed access to data on its computer network. In the end, the University agreed to pay a ransom of approximately one million euros (2020).

Four good practices to avoid email-related cyber-attacks

The preferred entry point for hackers on the Internet is email. And the massive growth in teleworking caused by the pandemic has increased the number of attacks, especially by ransomware. Indeed, the Experts Club of Information and Digital Security (Cesin) estimates that by 2020, 57 % of companies have been victims of a computer attack. A number quadrupled in one year.

However, it doesn‘t have to be that way! There are solutions to protect your company. This requires the adoption of several good practices, which we deliver in this article.

Good practice #1
Raising awareness among employees

The first thing to do is to communicate to your teams about the risks of cyber-attacks and the consequences they can have for the company. This means explaining how to recognise a suspicious email and the various precautions to take to secure access to their email. Your employees will be encouraged to set a secure password, limit the sending and opening of attachments, not click on links that seem suspicious, not divulge confidential information, check the identity of the sender, etc.

It is also important to stress the importance of notifying the IT department in case of a suspected fraudulent email. The reaction must be quick so that they can initiate the appropriate procedure before the virus spreads and causes significant damage.

Good practice #2
Safeguarding sensitive data

Since the implementation of the RGPD, cybersecurity issues have become even more strategic for companies. The security of access to the information systems and personal information must be guaranteed.

To secure data, it is essential to implement a rigorous password management policy. This is the first level of security for your employees' workstations. Passwords must be complex, difficult to guess, confidential and renewed regularly.

For greater security, set up your employees' workstations so that they lock automatically after a few minutes of inactivity. It is also essential to protect files containing sensitive data and to limit access to authorised persons only.

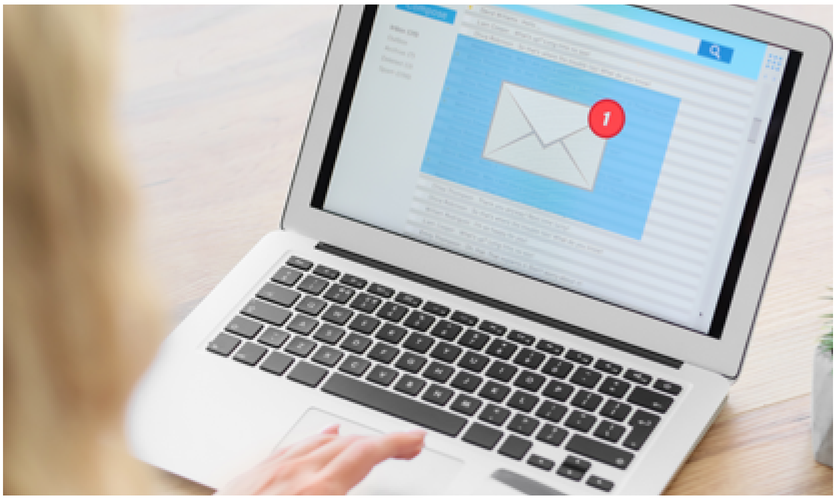
Still with the aim of securing the information systems, it is important to encrypt sensitive data such as those relating to health, payment information, etc. All these preventive measures go in hand with protection of the network infrastructure with the installation of firewalls, filtering routers, anti-intrusion probes, load-balancing systems and detection of DDoS attacks, etc.

Good practice #3
Keeping control of email traffic

Email is still the most used communication channel in the world. Users receive hundreds of emails a day. This is both stressful and inefficient, but it also has a significant impact on exposure to cyber-attacks. As our email security report shows, more than 75% of emails are unwanted.

This is why the control of email traffic is essential: it is necessary to ensure that fraudulent emails remain at the doors of the company's IS. But this filtering must be fine and precise so as not to eliminate valid e-mails that are relevant to employees.

This is why it is important to set up and constantly adapt filtering rules, to maintain white and black lists, to place emails that are not fraudulent but suspected of being commercial in a quarantine zone. Users will be able to access it so that they do not miss any important information.



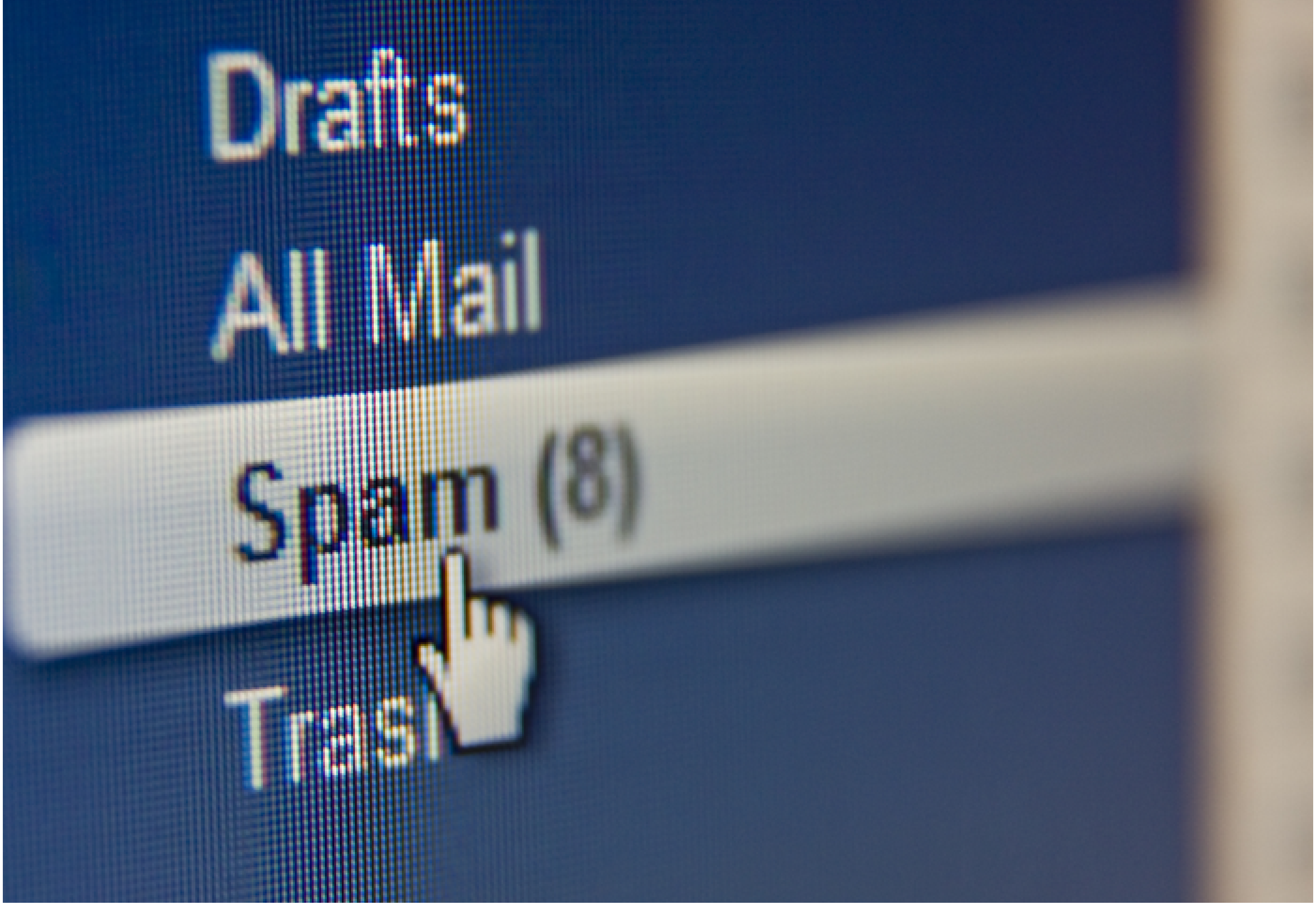
Good practice #4

Deploying an email securing solution

To strengthen the security of your business email, it is essential to deploy email protection software (such as antispam or antivirus). These solutions are updated as new cyber-attacks appear. They are perfectly adapted to the different professional email solutions, starting with Microsoft 365 Exchange. These tools filter spam by checking multiple criteria, automatically blacklist certain senders, protect your reputation (for sending mass emails, etc.).

Email solution providers offer native anti-spam solutions, but they are not always (or rarely) sufficient. It is thus essential to ensure a reinforced protection thanks to dedicated tools, such as Alinto Protect / Cleanmail. The advantages are numerous: email protection, cleaner email inbox, filtering finesse, quarantine management, time saving for email management...

To remind people of these four essential recommendations, do not hesitate to write down all the good practices in a document available to your employees. Communication and team awareness are also essential for the proper protection of your business email.



Why is the built-in antispam of email solutions not enough?

Many companies use the anti-spam software offered with their email solutions. They don't see the point of adding an additional solution. Some don't even use one! Yet this is a real concern for organisations as email is the main entry point for cyber-attacks.

In addition to raising employee awareness of the best practices for recognising fraudulent emails, it is important to strengthen the security of your professional email system. In many cases, the anti-spam software offered by your provider is not enough. We tell you why.[14]

Built-in antispam is not efficient enough

Anti-spam software built into email systems filters out unwanted email using general, predefined filtering rules. These rules are difficult to administer and are not easily adaptable to the needs of users and to the sudden appearance of new threats. It is therefore an incomplete protection of the email system, blocking emails from spam lists, which have dubious objects or attachments.

The proof: in 2016, AV Comparatives sent 127,800 spam messages to accounts held with email service providers. The detection rates were very low: 89.87% of the spam arrived at one of the providers. This shows that it is important to go beyond the basic versions - apparently free, at least at no additional cost - and to get a more powerful complementary solution.

The more powerful are very expensive

Of course, email providers offer enhanced, paid versions of their anti-spam software (such as Microsoft Advanced Threat Protection / Microsoft 365 Defender). These offer more advanced features. For example, they can be configured by the administrators (display, modification, configuration). It is also possible to create custom rules for each user, which will always take precedence over the global rules.

These versions also offer automated processes using artificial intelligence. They go further and identify commercial campaigns that escape first-level filtering. Dashboards are also available to analyse the evolution of mail traffic and the number of spam, junk mail, etc.

However, these solutions are quite expensive and are invoiced on the basis of the number of users. On average, you should count on several tens of Euros per month and per user. Do the calculation according to your number of employees: this is a significant amount for companies, which sometimes prefer not to use them. In this way, they leave the field more open to cybercriminals.

Antispam: what support does your email provider offer?

Popular business messaging providers are sometimes victims of their own success. The downside is that their support is not easily reachable or available. In the event of an incident, it is important to have access to efficient and responsive support. Moreover, it is often necessary to go through integrators to deploy these solutions, limiting direct relations with the vendor.

By working with a human-sized anti-spam solution editor like Alinto, you put all the chances on your side to benefit from a reactive partner, accessible and aware of your problems. This is a significant advantage when you know the consequences of an email unavailability or a cyber-attack. Make sure you get the right information before making your choice, as not all service providers offer the same level of support.

Even if the large professional email providers offer anti-spam as standard, it is essential to strengthen the security of your employees' email boxes. There is a wide range of complementary solutions available to you. To make the right choice, define a list of criteria that you consider essential: support, functionality, ergonomics, proximity, price basis, etc. Don't forget: it's the software that adapts to your challenges and not the other way around!

Five key features for your email security solution

You are convinced: you need additional protection from your professional email. However, it is difficult to choose from the of solutions available. Between the anti-spam solutions integrated directly into the email service and additional software, your mind is on the fence.

In our view, five features are essential. They must be offered by your future supplier. Here they are.

Feature #1

Filtering of incoming emails

Of course, your future email security software must offer you efficient filtering of incoming emails. This can be done in several ways:

- Reputation-based email filtering: filtering of known spammers, querying of international reputation databases...
- White list: selection of senders whose emails the company accepts.
- Blacklist: list of senders whose emails the company rejects.
- Content analysis: blocking of a message based on its content (analysis of words, links, images, attachments, etc.).

For even more agility and adaptability, choose a solution that allows you to modify, adapt, delete or add filters easily, in a few clicks and according to the needs of your end users.

Feature #2
Antispam and antivirus

In relation to the first functionality, it is important to choose a security solution equipped with a powerful anti-spam and anti-virus. Indeed, while the first feature makes it possible to ensure the legitimacy of the sender, the latter may unknowingly send spam or a virus. The message must therefore be analysed in depth. Many unwanted emails manage to get past the anti-spam tools built into email solutions and end up in your users' inboxes.

Choose a solution based on powerful technologies, which queries international shared databases, but also takes advantage of its own spam databases that will adapt to local semantics and submits emails to different antivirus programs for better filtering of cyber threats.

More precisely, in order for the software to define with accuracy whether the email received is spam, it analyses several elements of the email: links, subject, attachments, images, etc. according to set criteria.

Feature #3
Protection of your reputation

It is important that your domain name has a good reputation so that emails sent by your users, especially commercial ones, are not considered as spam. For this, a sender score is set up. It takes into account several elements such as the hard or soft bounce rate, opening rates, spam complaints, regular cleaning of your databases, the use of identification protocols and the quality of your emails (avoid attachments, images or objects that are too advertising).

The purpose of the sender score is to avoid being blacklisted and to increase the deliverability of your employees' emails.

Feature #4
The BCP (Business Continuity Plan)

The inability to access an email inbox can have disastrous consequences for business. However, this is what can happen in the event of a system failure or unavailability of an IT infrastructure.

This is why we advise you to choose an email solution with a Business Continuity Plan (or BCP). In this way, your users can continue to use their mailboxes via a backup webmail system, in complete transparency, and will not be affected by the unavailability of the mail server, even if it is in the cloud of a major player. None of them can guarantee or offer 100% availability.

In addition, as soon as access to the server is restored, the email exchanges made during the outage are re-synchronised with the messaging system so that no information is lost. A real bonus.

Feature #5
Integration with the existing environment

Beyond the functionalities, the ease of deployment can make the difference. Choose a email security solution that adapts to your work environment: email provider, hosting, customisation needs of rules according to users, autonomy of use of the solution, availability of APIs, etc.

This is essential to strengthen the protection of your messaging and to keep an independent administration. Whether on-premise or in the cloud, onsite or outsourced, your future solution must adapt to your requirements, not the other way around.

Of course, this list of «must have» features is not exhaustive. However, in our opinion, these are the essential criteria to take into account when choosing a security solution for your business email. If you would like to know more about this, please contact us.

What support is needed to deploy anti-spam system?

As we saw earlier, the capabilities of your email security software is critical. But there is another crucial aspect to consider: support. Whether it is during the design and scoping of your project, during the deployment of the solution or in the event of new questions downstream, you should choose a local service provider who acts as a true partner.

And that is what we offer at Alinto! Find out how we ensure the support of our customers at the heart of our solution.

Anti-spam software : expertise and support above all

There is no need to repeat it, the protection of your professional email is critical for your company. It is therefore important to call upon a partner who has it in his DNA and who has a deep knowledge of email security. And that is Alinto's strength.

For more than 20 years, Alinto experts have been accompanying companies in the management of their professional messaging systems. We meet their expectations, follow the evolutions and trends in terms of cyber-attacks and offer ever more advanced functionalities. We allocate 30% of our turnover on research and development to offer ever more effective solutions to secure our customers' email systems. Through several acquisitions of companies specialising in email security, we have all the skills and knowledge necessary to ensure the protection of your email inboxes, and beyond your information systems.

The support service is the keystone of our company. Thanks to a ticketing system, our experts are notified in real time of situations encountered by their clients. They can thus provide a response or take decisions adapted to the problem within a timeframe that takes into account the risks.

Deployment of anti-spam solutions: responsiveness is the key word

In connection with the customer support service, the Alinto consulting teams are at your side during all the stages of your project. Prior to the deployment by helping to frame your project. During the deployment, by accompanying you to install the software, and to configure the required functionalities. And post-deployment, with answers to your enquiries, the maintenance, the support...

We respond quickly to different needs, communicate efficiently between different departments in order to provide an adapted and fast solution. Our software, and hence your protection, gains from this agility. We know how troublesome it can be if your email service is interrupted, which is why proactivity is key for our services.

Beyond anti-spam : optimising management of the messaging system

To protect your business email, it is not enough to set up an anti-spam software, even if this is essential. It is important to look beyond this to optimise the management and protection of your emails. Therefore, choose a software that offers additional features.

At Alinto, we offer, in addition to anti-spam and anti-virus protection :

- An email archiving solution, useful for meeting the regulatory requirements. You choose what you want to retain and what you don't, you can change the rules, frequency... and are alerted before the emails are deleted.

- An SMTP mail relay to ensure that you send «clean» emails and do not jeopardise the reputation of your email domain.

- Email encryption, which secures outgoing emails with an encryption system, required in the exchanges in a number of industries. Only administrators are impacted by encryption, which remains totally transparent for users.

- Fax and SMS cloud services to provide a single solution for all your communication channels. Thanks to APIs or directly via emails, receive all the Alinto expertise to dematerialize your faxes and SMS.

Alinto also offers other services related to e-mail. With one common characteristic: proximity! You have a project or questions? Do not hesitate to contact us!

Conclusion

With the threat of cyber-attacks becoming increasingly sophisticated, protecting business email is no longer an option for organisations! And settling for standard versions of anti-spam software is no longer enough.

That's why choosing a business email protection software is the best option to ensure that you are on the safe side. It is also important to raise awareness among employees, to communicate about best practices on a daily basis and to monitor and anticipate cybersecurity trends.

About us

Founded in 2000, Alinto is a company specialised in the email business: email service in SaaS mode, anti-spam, email server... through several products:

- **Alinto Protect / Cleanmail:** the secure email relay that immunises against Internet risks by ensuring permanent access to emails.
- **Alinto Gateway / Serenamail:** The SMTP mail relay allows servers or applications to send emails to guarantee «clean» traffic.

Present in France, Switzerland and Spain, Alinto has more than 30 employees and provides a quality service to more than three million users. Thanks to its email services, more than (15) 20 million emails are sent every day.

Lyon (headquarters)
15 quai Tilsitt
69002 Lyon
+33 481 09 01 10

Barcelone
Avda. Diagonal, 434
08037 Barcelona
+34 91 005 29 64

Zurich
Gertrudstrasse 1
CH-8400 Winterthur
+41 52 208 99 66

Alinto

www.alinto.com