SMX

7 STEPS TO CYBERSECURE EMAIL

October 2021

EMAIL SECURITY IS HARD. GREAT EMAIL SECURITY IS EVEN HARDER.

Email is how the world does business.

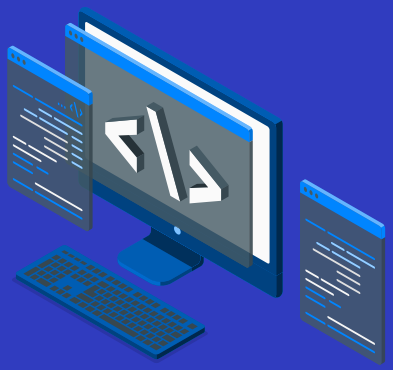
It lets every business and any business person send and receive information at a breathtaking pace. That ease of use also makes it the primary gateway for cyberattacks. It's the front door of your otherwise barricaded citadel.

While most business leaders know the risks in theory, it's not until something goes wrong that they really understand. Outages grind business to a halt, costing tens or even hundreds of thousands of dollars.

But on the flip side, security must be balanced with the need to maintain that easy exchange of information.

These are high stakes. With that in mind, here are the seven steps any organisation can follow to support teams to secure and defend email flow.

01.
Understand your current setup



Before you improve anything you need to know what you're improving.

Do you understand your current set-up? Now is the time to identify the staff members, mailboxes and information that need special attention. Start by documenting how email is currently used in your workflow, then get a handle on how and where your email assets are used.

HOW TO ANALYSE YOUR CURRENT SET-UP

- Identify specific users or mailboxes especially at risk, such as the finance team, senior executives and support mailboxes that might be phishing targets. Check they don't have email addresses published on public sites.
- Clearly document any regulatory or industry-specific compliance obligations, such as records retention or sending/receiving PCI or health records.
- Document the policies you have in place and how they help you comply with any regulatory obligations.
- Identify any requirements that aren't currently being fully complied with.
- Describe your mail flow and how it is embedded in your organisation's workflow.
- Ensure the general architecture is well-known and, if on-premise, that you know the versions and support info.
- Confirm that your provider is meeting all your requirements.

02.
Simplify your setup

The email security configuration of many organisations has grown over time, cobbled together in reaction to various security threats.

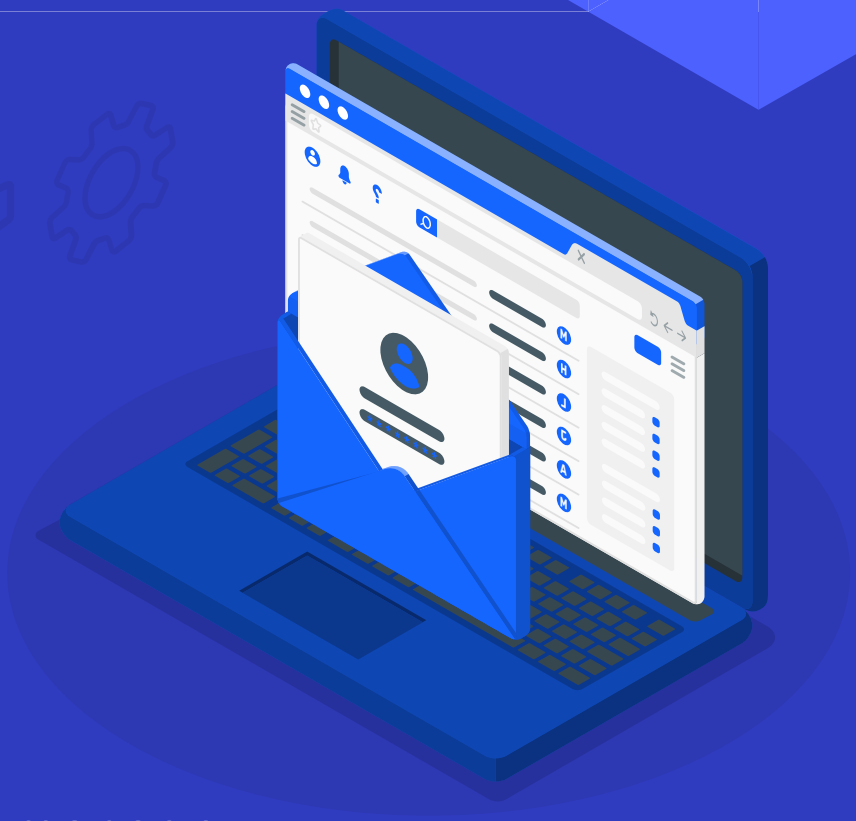
That means it's common for security configurations to contain obsolete rules or to cater for domains or groups of users that no longer exist. This isn't just inefficient and more easily exploited, it can also frighten support staff, making them unwilling or unable to properly support your email environment.

Simplifying your set-up changes that. Start by reducing the domains you still relay mail for and removing old or obsolete rules, especially those created for a specific malware outbreak. Malware signatures from historic outbreaks are well known by security vendors and can easily be detected and blocked by dedicated filters.

Employing DMARC should be a priority, and aggregating your sending sources helps with that. For some sites, that may mean a wider shift in how you manage email. For example, you may need to implement a policy to ensure staff send all outbound emails via the organisation's servers or cloud provider rather than via their ISP's SMTP submission service.

HOW TO GET A SIMPLER (AND CHEAPER) SET-UP

- Trim obsolete rules and policies, like those relating to historic malware outbreaks and users or workflows no longer employed.
- Remove MX records from domains used for web or promotional purposes and where no email is actually received.
- Aggregate your sending sources as much as possible.



03.

Put controls in place to manage your mailboxes, staff and data

Once you understand what mailboxes, staff and data you have – and the controls you want to put in place around them, you need to create rules to enforce them. This should include ongoing security awareness training for all staff and specific training for those most at risk of attack.

While your organisation's policies will be unique to you, they should be guided by some general considerations.

WHAT TO CONSIDER WHEN CREATING POLICIES

- Report and describe: ensure all policies that affect email clearly report and describe what they're doing. This could be a description of the individual rules in your admin console or in your security operations manual.
- Make use of directories: manage staff into groups and integrate Active Directory (AD) or similar to help ensure you're correctly capturing and classifying data.
- Inform staff: make sure affected staff know about the changes, and where to access support if something goes wrong. This will ensure smooth running and also opens the door to feedback in case things aren't working as expected.
- Conduct security awareness training: this is critical to improving your email security profile. For staff identified as potential phishing targets, this should also include phish threat training. This helps raise the awareness of email-borne threats and provides real-world examples of past attacks. This training needs to be constantly refreshed, to keep up with the ever-more-sophisticated tricks and techniques used by attackers.

04.

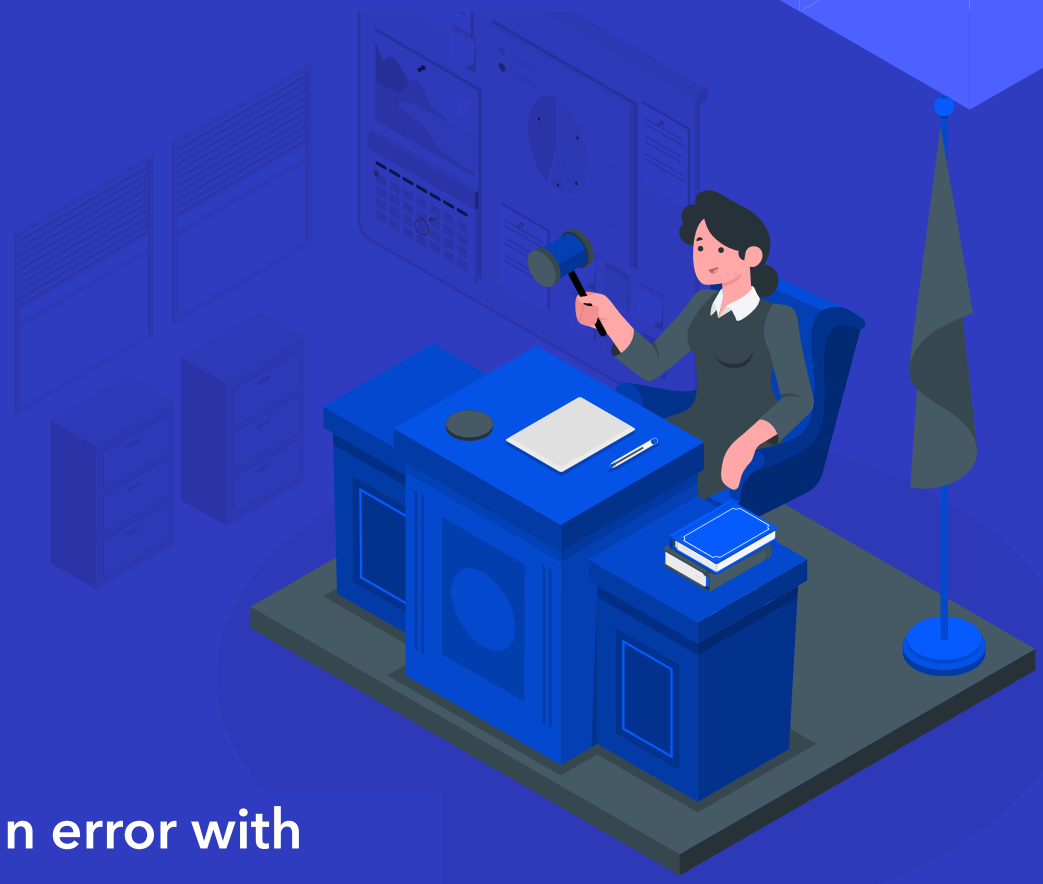
Secure your domain and email reputation

While most companies look hard at the emails that come into the organisation, they often overlook what's being sent. If anyone can send an email that appears to be from your business, you don't have control of your email reputation. Locking down who can send those emails puts you back in charge. And why is your domain reputation important? It's what determines whether emails sent out of your company will be accepted – if you have a bad domain reputation, your emails will be rejected, blocked or junked.

Recently, several new technologies – DMARC, DKIM and SPF – allow domain owners to control who can send email from their domains. This prevents bad actors from sending spoofed emails. DMARC also provides reporting tools to help with your deployment and refine your configuration post-deployment. Here's a more in-depth look into the history of DMARC – and its value to organisations.

HOW TO PROTECT YOUR DOMAIN REPUTATION

- Deploy DMARC, DKIM and SPF on your domains.
- Aggregate sending sources through your email security provider.
- Use a phased approach – you can apply DMARC policy to only a defined percentage of email from your domains as you roll it out, or authorise MTAs to report only on emails that fail your policy.



05.

Sidestep human error with modern tech

Email came well before the modern security mechanisms developed to overcome human error – which can have a huge impact on your business. Single sign- on (SSO) and two-factor authentication (2FA) can be applied to email, but those solutions simply don't occur to most organisations.

Deploying SSO and 2FA on your domain immediately improves your security. It's a fast, easy win.

How do they work? Using SSO for accessing third party services reduces the likelihood of credentials being stolen. 2FA provides token-based authentication mechanisms, which reduce the chance of fraud, data loss and identity theft.

While 2FA is easy to use, SSO stands out in that it secures applications while giving users easier access.

That improves productivity and reduces password fatigue.

IMPLEMENTING 2FA AND SSO

- Enable 2FA by proxy for applications that don't offer it with Active Directory. This means you can apply 2FA rules to users accessing applications with SSO active.
- Implement SSO for a better user experience and reduce the number of times credentials are sent over the internet.
- Deploy 2FA to improve security and ensure that even if credentials are stolen, they can't be used without the associated physical token or smartphone app.

06.
Outsource to specialist provider

Most organisations would benefit from outsourcing email security management to a specialist cloud provider. It's been industry best practice since at least October 2019, according to The Radicati Group.

That's because email is complex and highly visible, requiring suitably trained and experienced engineers to look after on-premise servers and appliances. That's nearly always more expensive than outsourcing, while also delivering a lower level of security and monitoring.

Outsourcing also increases the speed of updates to keep ahead of new attacks and techniques. Cloud service providers are constantly updating their engines and feature sets to combat the latest attacks.

WHAT TO CONSIDER WHEN MOVING TO OUTSOURCED EMAIL SECURITY

- Choose a provider physically located in your region – local providers will be more able to help you meet compliance requirements and will know of the locally targeted threats.
- Remember that even when you outsource your email security responsibilities you haven't outsourced your liabilities. That means it's key to keep an eye on the performance ofn your provider, whether that's a third-party audit or internal validation.
- Find a provider with a robust record of protecting organisations your size or larger.
- Ask other organisations in your sector for recommendations and experiences.
- Look for providers who offer access to timely critical "dashboard level" information.

07.

Expect to find gaps in your email security

Don't be fooled. No matter how much effort you put in, there will always be gaps in your email security. Sooner or later, they'll be found. The important question is, will the finder be in your team or someone with nefarious intentions?

Staying ahead of cybercriminals is an ongoing process and it starts with getting timely information to the right people.

Most providers will let you create scheduled reports to feed into your SIEM systems. This lets you analyse what's been happening at your edge, as well as what is coming out of your networks.

Some providers will also offer extra reporting relevant to different stakeholders. Reports for your network engineers, for example, might highlight email accounts that have received or sent the most threat emails, domains that are at risk or recommended configuration changes. Reports can also be provided for executive and general audiences to help explain the threat landscape in non-technical terms.

Additionally, DMARC's reporting and conformance tools provide information from external receivers relating to your domains. This critical information helps you see where your domains might be unprotected or where there might be other gaps in your email security.

HOW TO KEEP AHEAD OF CYBERCRIMINALS

- Integrate service provider reports with your reporting or SIEM systems.
- Ensure any reporting is meaningful.
- Assign responsibility for analysing and actioning these reports.
- Update your organisation's security configuration when any issues are identified.
- Document any updates for later reference.
- Perform audits of your organisation's security configuration regularly.
- Subscribe to your provider's mailing list to stay on top of the latest threats.
- Ensure your team knows how and where to access support from your provider.

"CYBERSECURE EMAIL: IT'S ALL WE DO."

About SMX

SMX is a cyber security company with specialist expertise in email. It's all we do. That means you get local expertise to help you secure your organisation's email. And when you protect your email, you're also protecting your brand reputation.

For more than 17 years, our in-house development team has been delivering that to hundreds of public and private businesses, offering training, support and the latest in tech solutions.

Our unrivalled email security encompasses multiple layers of protection, conforms with best-practice standards, and is data and workflow-driven.

This is amplified by strong partnerships with the likes of Microsoft, government agencies, M3AAWG and best-of-breed security vendors.

We protect around 25% of all Office 365 mailboxes in New Zealand and process 1/3 of all NZ's mail-flow.

Get in touch to learn more about how protecting your email can make your whole organisation more cybersecure.

Contact Us

Australia	1800 476 976	
New Zealand	0800 769 769	sales@smxemail.com
International	+64 9 302 0515	smxemail.com


SMX