A quick end to whaling and phishing at Genesis Energy

Genesis Energy, New Zealand's largest electricity reseller, has been a long-time SMX customer using SMX email filtering and the Custom Rules Engine to deliver email security and peace of mind for staff, freeing them from the hassle of dealing with time-consuming spam, malware and phishing issues. One of the key benefits they've found from the SMX service has been the smooth integration into their Microsoft Office 365 system, providing them with an extra layer of email protection. A bonus for Genesis has been the SMX reporting feature, giving them a competitive edge.

We provide Genesis with email protection for 1500 users across six domains around New Zealand, using SMX inbound and outbound filtering, and Custom Rules Engine for content control.

Genesis Energy's Security and Compliance Manager, Reyna Ramirez Montes, is responsible for the overall security of the organisation, and keeps tabs on the local and international cyber threat landscape. She has found SMX fundamentally important in helping her meet these requirements.

Genesis has used SMX inbound and outbound email filtering since 2010, and Reyna singles out the inbound filtering for specific praise – "The inbound filtering is excellent. We've had a good experience with how quickly SMX identifies issues and then resolves them," she says.

Genesis Energy gets a lot of spam, however almost all of it is intercepted by SMX. "We still get some spam coming through – it's impossible to stop it completely, after all – but SMX catches most of it."

Reyna estimates that spam accounts for 10-15% of the total company email that hits SMX's servers and she says the staff "don't know how lucky they are" that SMX is in place. "If they had to deal with that amount of spam in their inboxes, it would waste a lot of time. The inbound filtering allows us to be more focused on our customers' needs."

> "I would absolutely recommend SMX to other businesses. It's a powerful tool, and easy to manage. And we don't have to invest a lot of time or resources to manage it – it pretty much looks after itself. It just works"

Reyna Ramirez Montes
Security Manager
GENESIS ENERGY

> We can do so many different things with the Custom Rules Engine. We really value the flexibility and freedom the rules give us.
>
> **Reyna Ramirez Montes**

This is especially significant in the 200-strong Hamilton-based contact centre, where email traffic is high. Reyna says: "The contact centre teams get and respond to a lot of email every day. They need to receive the email as clean as possible." The SMX effect is hugely beneficial to staff productivity, she says.

Evolving email with the Custom Rules Engine

The Custom Rules Engine really is the game changer in SMX's email security offering, giving customers flexible and sophisticated content control, as well as data loss prevention. The beauty of the Custom Rules Engine is that it is constantly evolving to meet the demands of the changing spam and malware threat landscape, and rules can be customised to meet the specific customer needs.

When Reyna joined Genesis, the company's executive general management team (EGM) was experiencing regular phishing attacks. Something had to be done – and Reyna didn't need to look far, as the building blocks for an effective solution were already in place.

"We wanted to be more proactive rather than reactive. That's when I discovered we weren't using SMX Custom Rules Engine to its full potential. So, I contacted SMX support to get the rules configured in such way that we get real-time visibility of the threat landscape. Now we know what's happening and that allows us to respond accordingly."

Genesis implemented customised versions of the block executables and whaling rules, to give their staff an extra layer of email security. "I appreciated the way the SMX support team worked closely with us to make the rules work exactly the way we needed them to," Reyna says.

The whaling module ensures Genesis' EGMs are as protected as possible against whaling and phishing attacks. It enables them to identify employees that need whaling/phishing protection and restricts the number of addresses their EGMs (the 'Whales') can send email from. It inspects email headers to identify emails that are spoofing nominated executive names, and if the 'reply-to' or 'from' headers are not from allowed addresses, the rule will trigger and quarantine the email, and then redirect it to the Genesis information security team for inspection. "Therefore, we not only stop malicious attacks and can forget about them, we also inspect and understand the attacks, "Reyna says.

The block executables rule, used to prevent ransomware-type attacks (e.g. CryptoLocker), is applied to all users. This rule works by referencing a list managed by SMX's support desk to identify and quarantine common executable attachments, stopping them from passing through the SMX filters. Genesis also has a list of types and names of attachments that they want checked, so both lists combined are very powerful, says Reyna. If any of the attachments are detected, the email is quarantined, the recipient is notified and the email is redirected to the information security team for inspection.

> We like to be proactive and be aware of trends, and the SMX reports give us these insights, helping us develop our own intelligence around the threat landscape and informing the security strategy.
>
> **Reyna Ramirez Montes**

The Custom Rules Engine is easy to implement and very cost-effective, when compared to the potential losses that could be inflicted on an organisation.

Overall, the choice to use SMX has paid off for Genesis, both in the sophistication of SMX's security solutions, and in the direct assistance they've had from the SMX team in tailoring the program to work more efficiently for them.

Reyna says SMX's reporting capability is an added bonus, with her team using the reporting feature quite heavily, extracting logs weekly to better analyse and refine their online security set-up.