Case Study

mimecast

Renewi has 7000 employees securely emailing

Ransomware can jeopardize waste collection

No employee can do without ICT these days. Employees who spend large parts of the day on the road also need access to e-mail, for example. But especially on a small screen, a link in a malicious e-mail is quickly clicked. For 'waste-to-product company' Renewi reason to make e-mail security a top priority.

Waste does not exist. It is a striking credo for a company that has its roots in 'waste services'. Yet it is Renewi's conviction that it was created in February 2017 following a merger between Van Gansewinkel in the Netherlands and Shanks in the UK. According to the recycling company, all raw material streams have a value.

At a Glance

Renewi is a leading waste to product company that gives new life to used materials every day.

www.renewi.com

Industry:

Waste disposal

Number of Email Users:

7000

Objectives:

- Secure the email of all employees
- Ensuring business continuity

Results:

- Implementation of email security for all staff members
- Significant reduction in number of malicious emails
- Substantial decrease of notifications at the helpdesk

By giving used materials a new life, Renewi is working towards a world without waste. Of the 14 million tonnes of waste that Renewi processes annually in nine countries, more than 90% is recycled or used for energy generation. A nice percentage, but not enough for the merged company. Through

> **"The consultations with the Customer Success Manager are very valuable to us," concludes Birjmohun. "Only a monthly report doesn't say much yet. More important are the conclusions you can draw from such a report. I want to know where we can improve. The Customer Success Manager really helps us with that."**
>
> *Nick Birjmohun*
> *Compliance & Information Security Manager bij Renewi*

investments in new equipment and innovations Renewi wants to contribute even more to a sustainable world.

Safe use of ICT

ICT often plays an important role in these innovations, but also in the further streamlining of Renewi's internal business processes. For example, more and more 'blue collars' - including the drivers on the trucks - have access to ICT facilities such as e-mail and Renewi's human resources portal. That number is being expanded step by step.

Eventually, all 7000 employees must have an e-mail address. Office staff and other employees.

"The use of these resources must be safe," says Nick Birjmohun, Compliance & Information Security Manager at Renewi. An error, such as accidentally clicking on a link in a malicious e-mail, is quickly made. For example, studies show that 90 percent of cyber attacks start with human error, and 90 percent of them happen via email. "Most of the cyber attacks come in through e-mail. For this reason we want to protect ourselves against ransomware and phishing attacks."

"A ransomware infection could jeopardize our business continuity," continues Birjmohun. "We can still rely on paper processes for a short period of time. However, if the problems persist for a longer period of time, waste collection is at risk and there is a risk that the business will come to a standstill". Renewi wants to avoid this in view of the crucial role it plays for companies and municipalities.

E-mail security

"Unfortunately, we've already had a major phishing incident," says Birjmohun. "An attacker had managed to penetrate an employee's account via a phishing email. When we tracked down the intruder, he had already hacked into the accounts of 25 colleagues. The criminal had been inside for two weeks."

Birjmohun doesn't know what the target of the attacker was. "Possible financial gain. Maybe he was trying to falsify invoices, or intercept bank transactions. It did make it clear to us that we had to take extra steps in the area of e-mail security, on top of the standard security measures that Microsoft Office 365 already offers us."

Mimecast S1

Together with partner Cegeka, Renewi evaluated three e-mail security solutions. "Mimecast S1 was the best in the proof of concept", Birjmohun looks back. "Mimecast caught significantly more malicious e-mails than the competition."

For extra protection - if, for example, a phishing email does pass through security - Renewi implements multifactor authentication (MFA). In addition to the username and password, the user then needs an additional factor such as an SMS code to log in. Cybercriminals who only know username and password using a phishingmail will still be left empty-handed.

Smooth project

Renewi deployed Mimecast S1 for initially 5000 employees, and then gradually rolled out the email security solution to the remaining employees. This second group consists mainly of non-office staff. They are given access to the company's ICT facilities in groups.

According to Birjmohun, the commissioning of Mimecast was not a big deal. "This was a project with great impact because it touched the entire mail environment. But the implementation went quite smoothly. There were actually no major issues. Together with Mimecast and our outsourcing partner, we drew up the schedule, carried out activities and held regular operational and tactical meetings to monitor progress. It all went very smoothly.

Customer Success Manager

The first experiences with Mimecast S1 are also positive. Birjmohun: "I see a clear decrease in the number of malicious e-mails coming in. I also notice this in the number of reports to our service desk. Together with Mimecast's Customer Success Manager we are also looking at how we can further improve the deployment of S1. For example, she helps us keep our security settings up to date so that we are always protected against the latest threats".