Wyntec
stress free IT

CUSTOMER SUCCESS STORY

Cyber criminals leverage routine purchase order to steal $30k

Customer introduction

The client is a large product sales and distribution business. Due to the client's diverse and broad range of global suppliers, they are frequently tasked with issuing a large quantity of daily purchase orders to suppliers for products to deliver quality solutions for their significant customer base.

The incident

Conducting such a large enterprise with a vast network of external suppliers is no easy feat. It potentially places a bullseye on them for vulnerability-seeking cyber criminals like in our client's case.

The organisation worked with known suppliers for many years, and communication and orders were primarily conducted comfortably over email as the go-to source of their routine correspondence and operations. Whenever a purchase order was sent to a supplier soon after, the accounting department would typically receive an email requesting the associated payment deposit be made, which would then be actioned.

The only indicator of a change to this routine was a request to make a specific routine payment to a different bank account. Nothing seemed unusual when reviewing the email trail of correspondence leading up to this request, so an approved payment of $30,000 was made to the new account from the well-known supplier.

Several days later, when following up with this supplier for an ETA, the supplier had not received the payment, which was the first sign of this particular cyber breach. The payment had been made directly into a cyber criminal's account.

Enter Wyntec's Security Team

From the client's perspective, no amount of technology would have stopped this problem from happening. This was a systematic failure of their own human-based internal processes and management. There were no policies or procedures to flag this requested account change request; therefore, this routine payment was a prime target for the hackers to target.

The Wyntec Security Team was contacted to identify what had happened and rectify the failings of the customer's processes. Upon review, it was clear the supplier's email system had been compromised, and the attacker had utilised this external organisation's manager's account to action the theft.

The hackers patiently monitored the account for an unknown period of time and then struck when the opportunity was right. The supplier's email users were unaware of this account hijacking as the messages had been moved and deleted as they arrived. The attacker was utilising their own email client to conduct their communications with numerous clients, including our client.

Outcomes

With 95% of known cyber attacks* caused by human error, Wyntec knew the solution would need to focus heavily on the customer's staff cyber awareness and risk mitigation best practices.

Policies were developed for them around how to manage supplier requests, including Bank Account change requests. This ensured all changes made to the ERP Systems would not only be documented but need direct approval, not just via the sent invoices, but with details already on file.

This incident also highlighted the importance of ensuring multi-factor authentication is enabled on all email accounts. As seen in the supplier's case, this would have inhibited their breach with additional control over accounts and attempts at compromising them.

Is it time you started taking cyber awareness seriously?

Get in touch to explore the best path forward for your organisation.

Contact us