AuthN by IDEE

CASE STUDY

Udo Gärtner Deploys AuthN by IDEE MFA Overnight after Breach

Major breach with steadily accumulating costs is swiftly abated with phish-proof MFA - deployed in just 15mins.

GRTNR IT

Udo Gärtner is a Managed Security Services Provider (MSSP), based in Hannover & Munich, Germany.

Attack on Major Supply Chain

Udo Gärtner's customer is a major supply chain partner in the food and drinks industry and connected to one of Germany's largest retailers. A security breach in one part of a supply chain has the potential for far reaching and devastating impacts well beyond the original source and can serve as an attack vector to further third-party targets. And this is exactly what was attempted.

The Incident

The successful attack hit the customer's **Microsoft 365 (M365)** accounts. Third party email recipients began to receive cleverly designed phishing emails and legally binding contracts, apparently, from the customers' own domain. The attack was sophisticated, using masterfully constructed DocuSign forms to fool its recipients into giving up vital data.

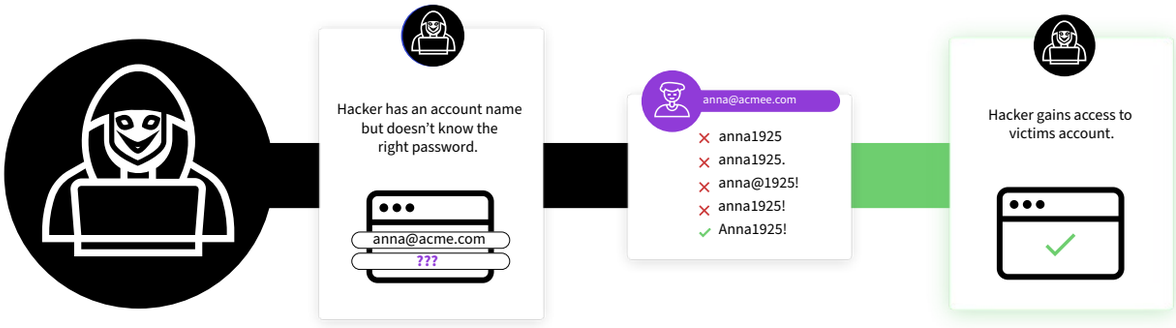
Research & Troubleshooting

As soon as the issue was reported, Udo Gärtner got to work. They reviewed the emails. They completed an urgent analysis into the customers DNS records, authentication methods (SPF and DKIM), and performed email forensics. They needed to see whether the emails were sent from outside of the customer domain or whether the email had been sent directly from the customer's M365 account. Unfortunately, it was the latter. This meant that the customer's M365 account had been breached.

After further research, it was discovered that there had been numerous login attempts on the server and that the account had fallen victim to a brute force attack – a popular tactic used by cyber criminals.

How Does a Brute Force Attack Work?

A bruteforce attack is possibly one of the oldest and crudest attack methods used by cybercriminals to hack into a victims private account. It can be incredibly effective, literally using 'brute force' to force a way in. It works by repeatedly hitting a known account with different password combinations until a match is found. With the correct password, the attacker gains full access. This is usually carried out with the use of software which can be leveraged to calculate login credentials, encryption keys or gain access to private or hidden webpages - simply by a process of trial and error.



Heavy Impacts

The impact of the attack were severe, with email traffic being completely blocked between the customer and one of its most important clients. Trading was effectively suspended with an immediate loss of revenue.

With these types of attacks, the financial impacts, the disruption to business and the loss of reputation is often vast. A swift and robust resolution was immediately required, not only to resume business but also to help restore confidence and secure all communications.

Overnight Protection – 15 Minute Phish-proof MFA deployment

Udo Gärtner deployed location-based IP blocks, and within just 24 hours of the breach, had also implemented phish-proof MFA AuthN by IDEE.

AuthN can be deployed in as little as 15 minutes and protects against all MiTM (Man in the Middle), credential phishing, and password-based attacks. Email traffic swiftly resumed, and revenue began to flow once again.

Udo Gärtner & AuthN:

A phish-proof future as Udo Gartner and it's customers kiss goodbye to password-based attacks.

Unfortunately, attacks like this are not rare and this was not an isolated incidence. This attack was attempted on multiple M365 accounts managed by Udo Gärtner and as a result, Udo Gärtner has now decided to implement AuthN as the standard for all current and future accounts.

As an MSSP, the company simply cannot risk the liability for customer damages, and it is vital to have one hundred percent confidence that customers won't be phished.

90%

of all attacks are caused by human error such as phishing according to a 2022 whitepaper of Munich RE.

Companies can protect their people, their networks and their entire ecosystems by just deploying AuthN by IDEE. With AuthN credential phishing & password-based attacks are not possible! If you are an MSP, or a Microsoft Sales professional, AuthN is now available for automatic deployment directly from the MS Azure Active Directory and provides margin-rich opportunities beyond the standard E4 & E5 licenses. It would also have prevented this attack!

Get in touch now for further information on how we can help.

IDEE

AuthN by IDEE enables people, organizations, and systems to connect privately, securely, and safely using the worlds-first passwordless and 100% phish-proof MFA. It stores zero personally identifiable information from any user, organization, or device. AuthN uniquely solves the most urgent and age-old industry problem of identity-based attacks with frictionless, easy-to-adopt solutions, deployed in just 15 minutes.

getidee.com
hello@getidee.de
@IDEEAuthN
/idee-gmbh/