Compromission de la messagerie en entreprise

Identifier les menaces

Les attaques par e-mail visant les entreprises varient désormais grandement en complexité, en volume et en impact. Voici donc quelques informations clés pour vous permettre de repérer les menaces avant qu'elles ne causent des dommages.

Dans le cas des attaques BEC, les cybercriminels usurpent l'identité d'un employé afin d'escroquer l'entreprise, ses collaborateurs, ses clients ou encore ses partenaires.

Dans la plupart des cas, les attaquants concentrent leurs efforts sur des employés ayant accès aux finances de l'entreprise ou à des informations personnelles, les poussant à réaliser des virements bancaires ou à divulguer des informations sensibles.

Ces attaques utilisent des tactiques d'ingénierie sociale ainsi que des comptes compromis, généralement sans avoir recours aux pièces jointes ou liens malveillants associés aux e-mails de phishing classiques.

Les attaques BEC peuvent user de l'autorité d'un supérieur afin de susciter une réponse. Les e-mails semblent ainsi souvent être envoyés par le PDG de l'entreprise lui-même ou par un cadre dirigeant.

Voici comment éviter de tomber dans le piège des attaques BEC :

- Méfiez-vous si vous ne recevez pas habituellement d'e-mails de supérieurs hierarchiques.
- Gardez votre calme, même si l'e-mail indique une certaine urgence.
- Vérifiez la légitimité de l'e-mail en contactant l'expéditeur.
- Signalez l'e-mail à votre responsable ou à l'équipe informatique si vous suspectez une fraude.

Exemple

Hi {email:firstName}

Need your help asap. Someone new at our bank accidentally blocked our payroll account and needs us to verify our information.

Pain in the behind, I know, but could you visit the link below and just make sure our information is correct? We can't make payroll without it. I tried the link but the hotel wifi security settings won't give me access.

http://www.chasebanked.com

Thanks much for taking care of this right away—I appreciate the assist as much as all of us appreciate getting paid on time.

Geez, what a stupid mistake! I'll make sure you get a shout out to senior management for helping fix it.

Let me know how it goes, okay?

Chief Financial Officer
Office of the CEO

◀ Business email compromise scams usually involve urgent requests from 'higher-ups' in an effort to get targets to respond to authority.

◀ A fake domain name, easily overlooked, leads to a fake website that will track and keep account details.

◀ The promise of recognition by senior management is a strong incentive to engage.

◀ A scribbled signature without the printed counterpart is an attempt to look authentic.