

# Self-Service Passwort Reset – Zwei Fliegen mit einer Klappe



**Stephan Halbmeier**  
Product Specialist | Specops Software


# Vom Ethical Hacking zum größten Cyber-Security-Assessment Anbieter in Europa



# Anforderungen an Kennwörter

1. Passwörter müssen lang sein!
2. Passwörter brauchen nicht komplex zu sein!
3. Passphrasen!
4. Privilegierte Konten mindestens 15 Zeichen!
5. Kompromittierte Passwörter blockieren!
6. Einfach zu erratende Kennwörter nicht zulassen!
7. Unterschiedliche Regeln für Standard -und Admin Accounts!
8. Typische Muster verhindern!
9. Kein Ablaufdatum ist vielleicht keine gute Idee...



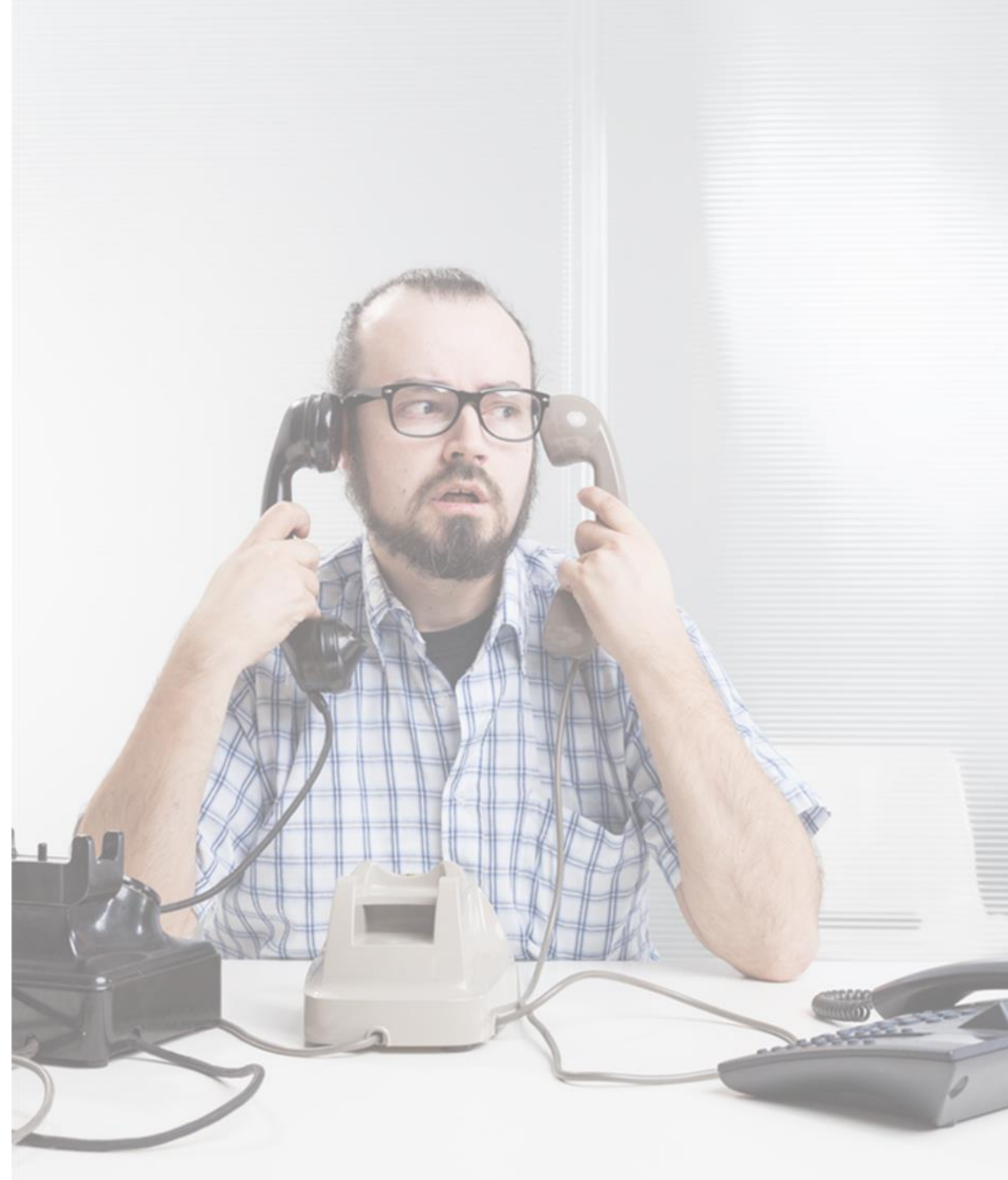


“Anfragen zum Kennwort  
Zurücksetzen machen 40%  
des Call-Aufkommens aus.”

# Social Engineering @ServiceDesk

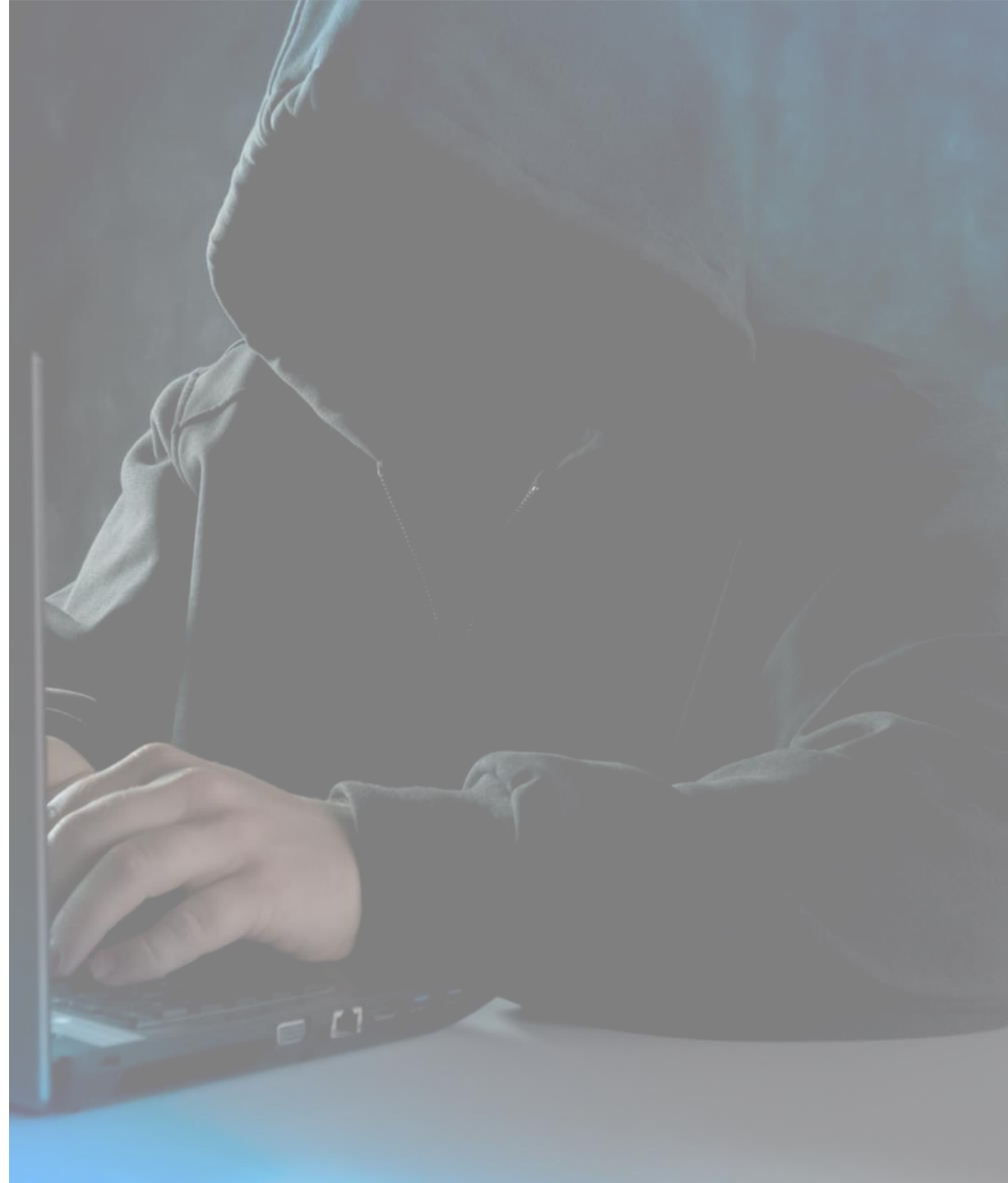
*„Beeinflussung von Menschen mit dem Ziel, sie zu bestimmten Verhaltensweisen, Preisgabe von vertraulichen Informationen, dem Missachten von Prozessen oder Umgehen von Schutzmaßnahmen zu bewegen.“*

*Eine klassische Methode, um sich unautorisiert Zugang zu einem Netzwerk zu verschaffen, besteht darin, den Servicedesk anzurufen, sich als eine andere Person auszugeben und ein **neues Passwort** zu verlangen.*



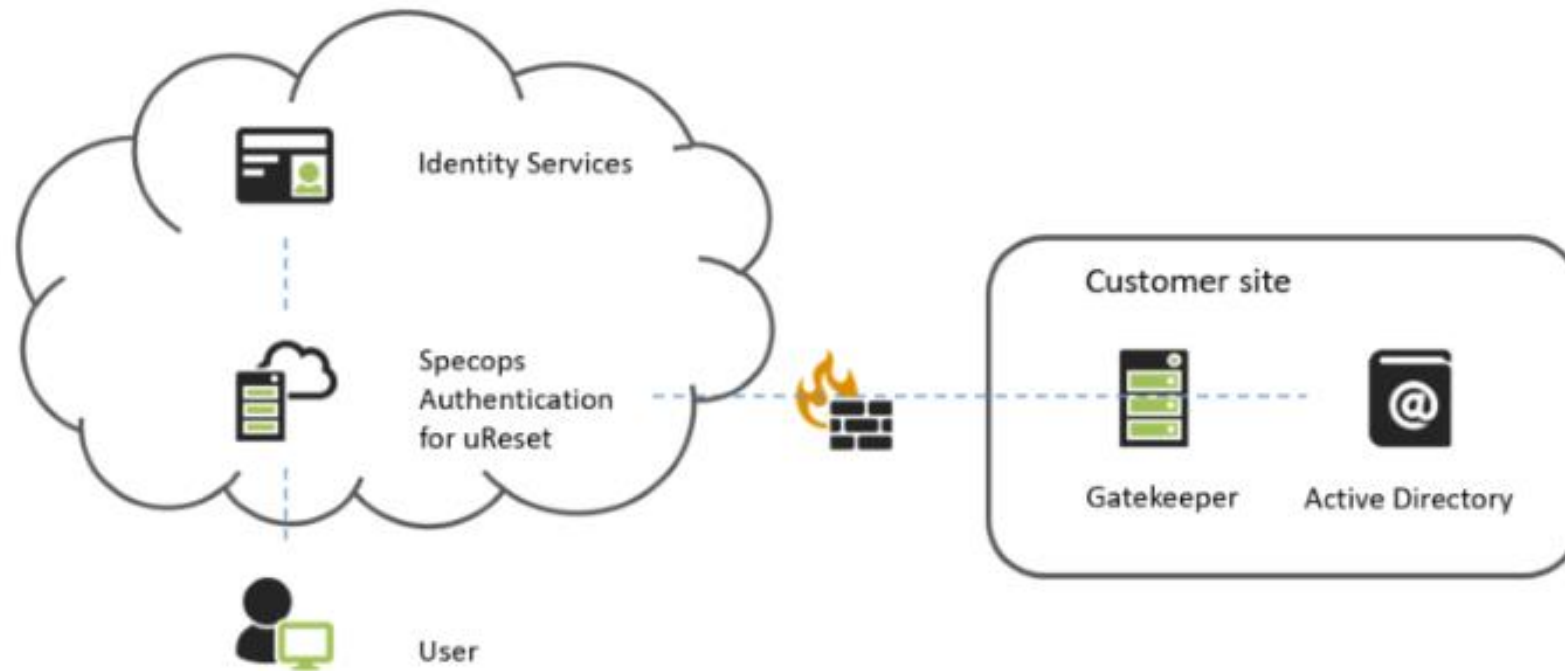
# Herausforderungen

- Anwender werden Kennwörter häufiger vergessen
- Produktivität der Anwender darf dennoch nicht beeinträchtigt werden
- Effizienz des Service Desk soll sich kontinuierlich verbessern
- IT ServiceDesk bleibt verwundbar für Social Engineering





# Specops Authentication Plattform für uReset & Secure Servicedesk





# Demo Specops uReset & Secure ServiceDesk



# Vielen Dank für Ihre Aufmerksamkeit

Für weitere Fragen zum Thema: <https://specopssoft.com/de/kontakt/>

Produkt-Demo: <https://specopssoft.com/de/produkte/specops-password-policy/>

Oder per E-Mail: [stephan.halbmeier@specopssoft.com](mailto:stephan.halbmeier@specopssoft.com)