

exccon

Experience Day 2018 München

BOMGAR™

ITSM und
sicherer
Umgang mit
Privilegierten
Benutzerkonten

Elmar Albinger · 17. Mai 2018

Agenda

- ▲ **Bomgar**
- ▲ **Umfrage**
- ▲ **Was sind Privilegierte Accounts**
- ▲ **Service Desk und Privilegierte Accounts**
- ▲ **Lösungen**



About Bomgar

The fastest, most secure way for experts to access and support the systems that need them.

- Trusted by more than 15,000 Companies
- 13+ year history of innovation
- 300+ Employees across US, EMEA, & APAC
- Leader in secure remote support and access management
- #1 in Enterprise Remote Support, according to IDC



What Do We Do?

Bomgar's Secure Access solutions enable customers to easily support people, access and protect endpoints, and defend privileged credentials, in order to fight cyber threats and speed business performance.






How many of you manage or are part of a service desk that supports internal employees?



**When supporting users, do
you use accounts that have
Workstation Admin privileges?**



**Do you use local accounts or
domain accounts in a
Workstation Admins group?**



**Could you still do your jobs
if you no longer had admin
credentials?**

Privileged Accounts are the Prize

▲ What are they?

- “Administrator” of the local computer
- “Superuser” used to perform administrative tasks
- Built into every IT application and system
- Sometimes shared among several people

▲ Why are they so problematic?

- They are all powerful
- They are shared, or stored insecurely
- They are anonymous

But, we can't live without them!



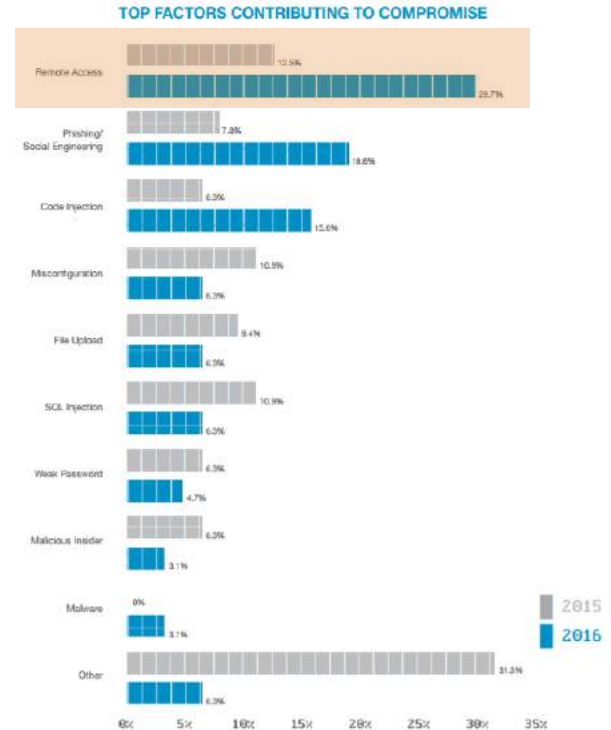
Cyber Breaches Show No Sign Of Slowing Down



- Targeted attacks on corporate IT networks have increased in scale and public visibility
- Phishing tactics are increasingly sophisticated and often involve social engineering
- Hacker objective is to bypass perimeter security, by stealing legitimate credentials to gain access

Remote Access is #1 Method of Compromise

- Extremely easy for threat actors to find unsecured remote access pathways
- Most security organizations don't have visibility into all of the remote access pathways into their networks
- Different teams & external vendors using their preferred tools
- No centralized monitoring or auditing

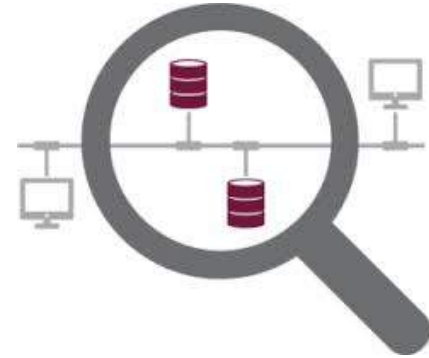


81% of Hacking-related Breaches Leveraged Stolen and/or Weak Passwords

- Privileged credentials are highly targeted “keys to the kingdom”.
- Admin passwords are often shared across teams.
- Many organizations forget about privileged credentials used by service desks, service accounts, app to app, third-parties, etc.



Bomgar ITSM Integration - ServiceNow



Discovery

Recommendations

- ▲ **Secure Credentials in an Enterprise Password Vault**
- ▲ **Randomize passwords of Local Administrator Accounts**
- ▲ **Rotate Passwords after each use for privileged Domain Accounts**





DEMO

BOMGAR™

CONNECT FEARLESSLY WITH SECURE ACCESS SOLUTIONS

Vielen Dank

Merci

Thank You

Grazie