CYBERARK®

EBOOK

AN ASSUME-BREACH MINDSET:

4 STEPS TO PROTECT WHAT ATTACKERS ARE REALLY AFTER

THINK LIKE AN ATTACKER

Traditional perimeter-based IT security models conceived to control access to trusted enterprise networks aren't well suited for today's world of cloud services and mobile users. Savvy attackers can breach enterprise networks and fly under the radar for weeks or longer. The 2020 SolarWinds supply chain attack went undetected for nine months, impacting over 18,000 organizations.

Threat actors are always finding new and innovative ways to penetrate networks, steal data, and disrupt business. It's not a question of if a breach will happen, but when. Cyberattacks can damage your company's reputation and result in costly regulatory fines, lawsuits, and revenue loss. The average total cost of a data breach exceeds $3.8M.*

It's time to adopt an "assume-breach" mindset to detect and isolate adversaries before they traverse your network and inflict serious damage. An assume-breach mindset means thinking like an attacker.

If, like us, you spend a lot of time helping organizations prevent and respond to attacks and breaches, you get to know a lot about how attackers think. So in this guide, we're using what we've learned to help you protect your organization against the most common attack paths attempting to compromise your most critical assets.

Listen to
Shay Nahari
Director Red Team:

Assume breach | Think like an attacker

Contents

* IBM Security, Cost of a Data Breach Report, 2020, https://www.ibm.com/security/digital-assets/cost-data-breach-report/#/

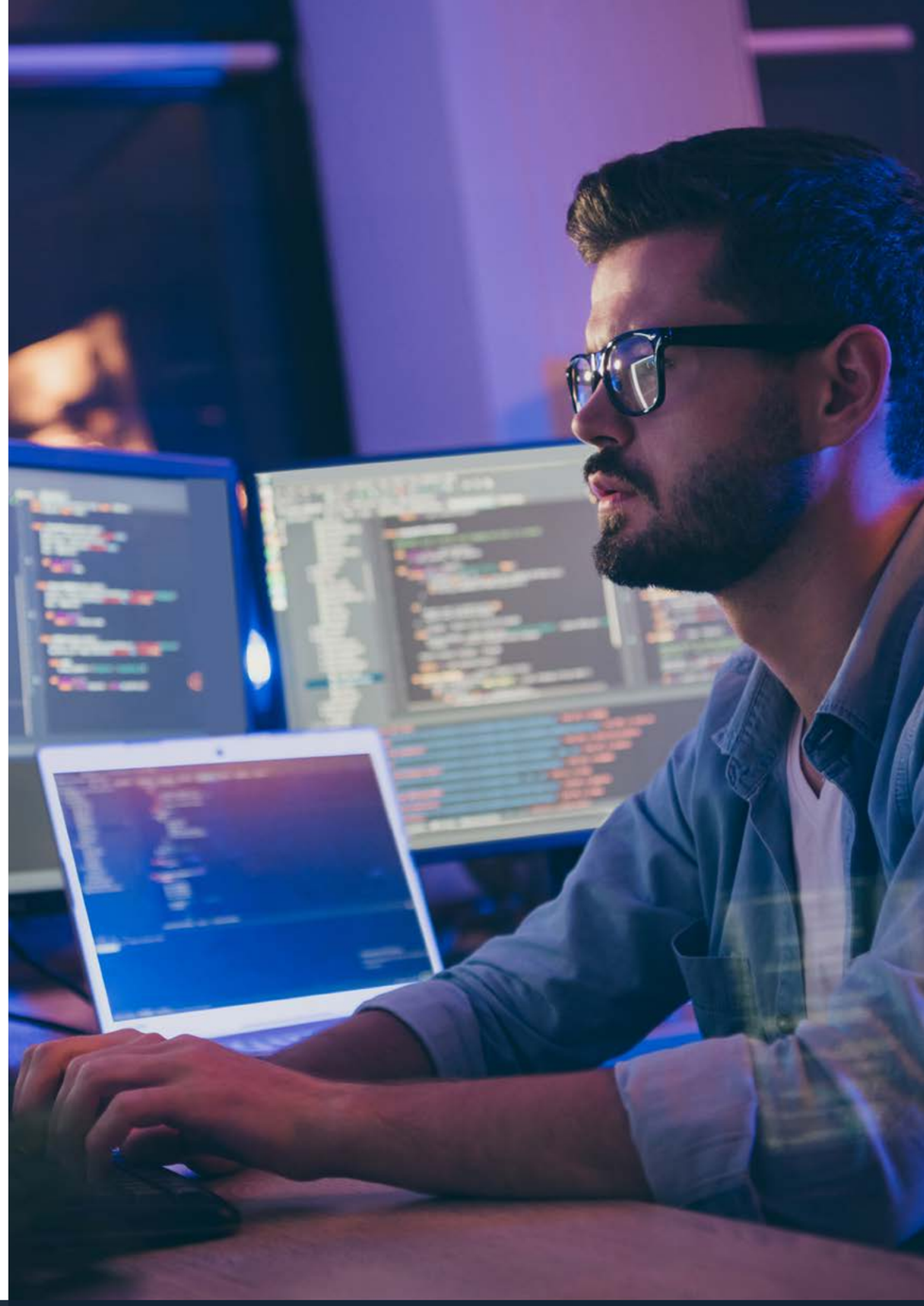
ADOPTING AN ASSUME-BREACH MINDSET

By adopting an assume-breach mentality and thinking like an attacker, you can efficiently identify suspicious activity, restrict lateral movement, and contain threats. An assume-breach mindset requires a defense-in-depth approach to security. By implementing multiple layers of defense, you can improve your security posture and mitigate risk.

Now is the time to take a fresh look at your security portfolio. Augment existing controls like endpoint detection and response tools, next-generation anti-virus protection solutions, and application/OS patching best practices with cloud detection and response tools, and zero-trust, identity-based security solutions. 79% of enterprises have experienced an identity-related breach within the past two years* and 80% of breaches tied to hacking involve the use of lost or stolen credentials.**

Identity-based security controls are critical for detecting and thwarting advanced attacks. Bad actors often exploit privileged identities in particular – to steal data or wreak havoc. In fact, nearly 100% of advanced attacks involve compromised privilege credentials.

Privileged Access Management (PAM) should be considered at the core of a defense-in-depth approach that is geared to protect critical infrastructure, safeguard confidential data, and making the most of your technology investments.



* Identity Defined Security Alliance (IDSA), The State of Identity: How Security Teams are Addressing Risk, December, 2019, https://www.idsalliance.org/how-security-teams-are-addressing-risk/

** Verizon, Data Breach Investigations Report, 2020, https://enterprise.verizon.com/en-gb/resources/reports/dbir/

ZEROING IN ON PRIVILEGED ACCESS MANAGEMENT

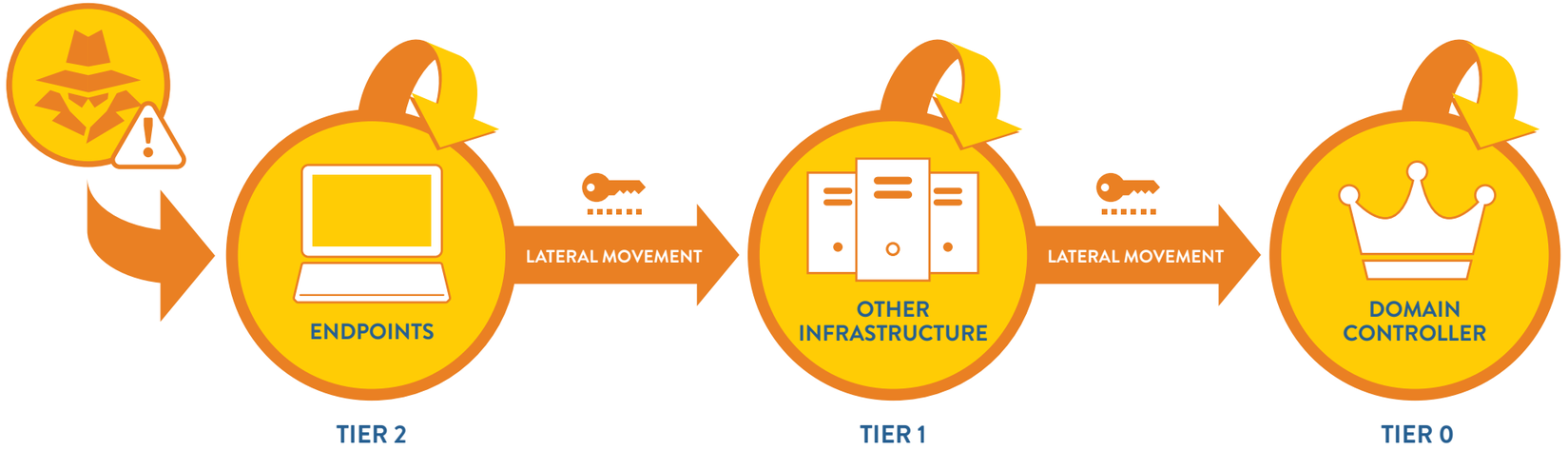
Would it surprise you to know that, as a general rule, your organization will have three to five times more privileged accounts than the number of people you employ? They comprise:

- **System access** accounts that come by default with servers, workstations and applications (for example, Windows administrator accounts, root accounts in UNIX, and Oracle SYS and SYSTEM accounts), and give 'all-access' privileges to the relevant system.
- **Technical access** administrative accounts, created by your organization so your people can do their jobs (for example, accounts for IT operations, support and development). This is typically your largest set of privileged accounts, but attackers are not equally interested in all of them. Their primary targets are the most powerful ones, especially domain administrator accounts.
- **Application access** accounts, created so that machines can access systems and data on other machines, usually to support process automation. These are non-interactive, machine-to-machine accounts.

You can't flip a switch to protect all of these, all at once — you need to prioritize the work required, so as to achieve the greatest reduction in risk as quickly and efficiently as possible. This is where it pays to know how attackers think and act.

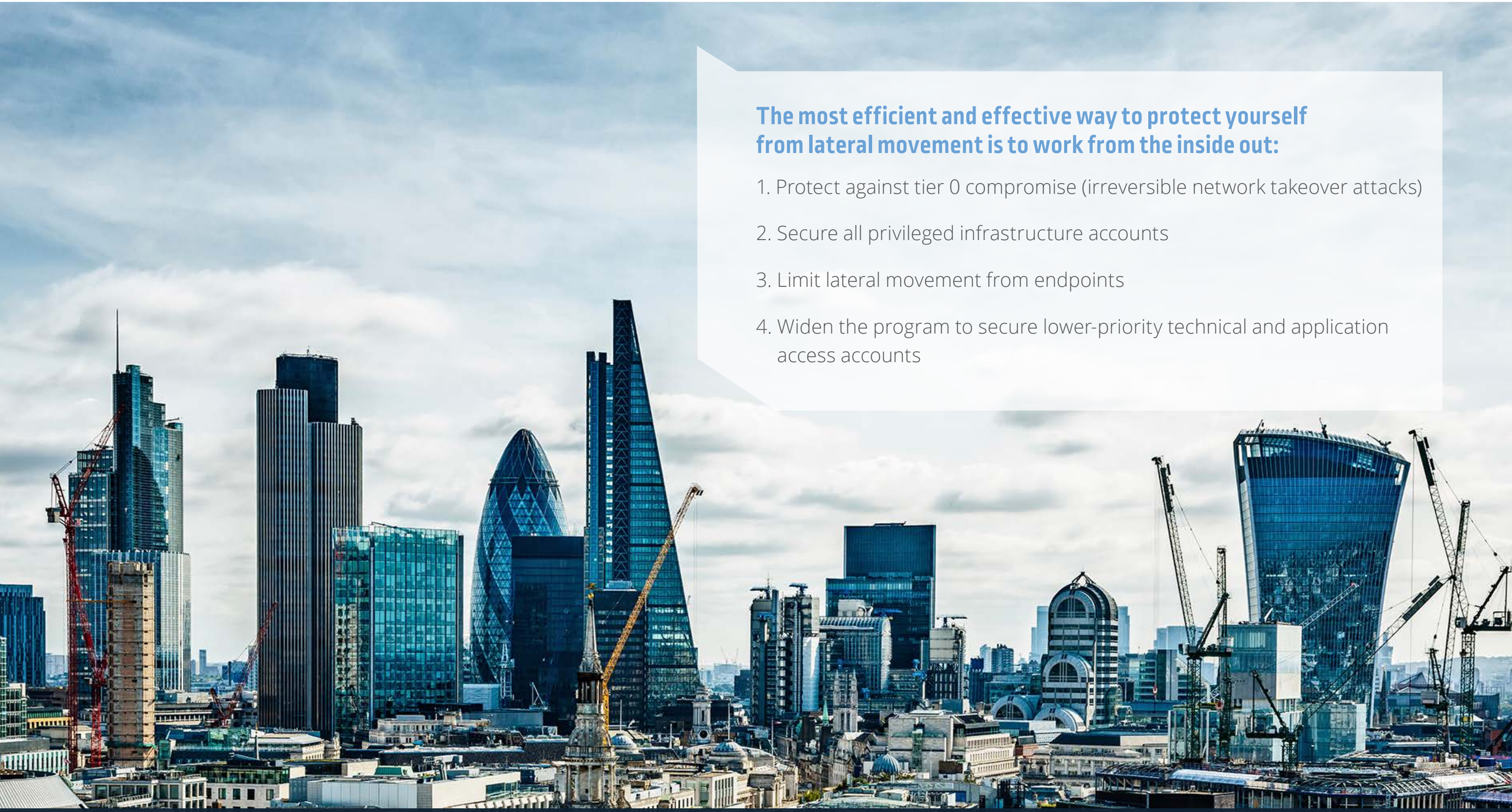
KNOW WHERE TO START:
NOT ALL PRIVILEGED ACCOUNTS ARE CREATED EQUAL

The jackpot for an attacker is your most powerful technical and system accounts: the administrator accounts that provide access to critical assets, such as Active Directory domain controllers and other high-level AD domains.



To get to these, attackers target accounts accessible from end-user devices (tier 2, where the compromise initially starts) and work their way from there towards more powerful accounts which themselves usually give access to sensitive data (tier 1 system and technical accounts).

This lateral movement may leverage system accounts, because they're often set to the same password across similar devices (for example, same local administrator password on endpoints). Your most powerful technical accounts come into play as the attacker gets deeper into your network, aiming for the systems that give control over all other systems (tier 0).



The most efficient and effective way to protect yourself from lateral movement is to work from the inside out:

1. Protect against tier 0 compromise (irreversible network takeover attacks)
2. Secure all privileged infrastructure accounts
3. Limit lateral movement from endpoints
4. Widen the program to secure lower-priority technical and application access accounts

1. PROTECT AGAINST TIER 0 COMPROMISE

Think like an attacker

"If I can compromise the Kerberos system that authenticates Active Directory accounts, I can do anything I want and nobody will know. They'll pretty much have to rebuild from scratch to get rid of me."

How they do it

The most common (though not the only) security lapses we find at tier 0 level are:

- Allowing access from tier 1 or 2 systems to tier 0 systems
- Use of single factor authentication for domain administrator accounts
- Failure to change domain administrator account passwords frequently enough

These lapses give attackers openings to exploit, such as capturing residual password hashes from long-lasting domain administrator passwords.

Listen to
David Higgins
Technical Director

Assume Breach | Where to Start

How to reduce the risk

As a matter of priority you'll want to block access to tier 0 assets from accounts managing tier 1 and 2 assets. If, for example, one employee needs to manage a mix of tier 1 and tier 0 assets, they should do so from different privileged accounts, each of which has access only to its own tier.

In parallel, choose a privileged access management (PAM) solution, preferably one with integrated multi-factor authentication support. This will enable you to generate a unique one-time password for every use of a tier 0 account, eliminating much of the danger.

2. SECURE ALL PRIVILEGED INFRASTRUCTURE ACCOUNTS

Think like an attacker

"If I get access to the right default infrastructure account, I can take ownership of an entire technology stack — and all the sensitive data it holds. Even better, I'll probably be able to use the same credentials to access other, similar infrastructure including CI/CD systems!"

How they do it

As with tier 0 accounts, the main exploitable issue here is with passwords for default system accounts that are only infrequently, or never, changed. The issue is exacerbated by the sheer number of these privileged accounts across your Windows, Unix/Linux, Cisco, SQL, Oracle, cloud and other systems. Even worse, because these are accounts shared among multiple users and teams, they are often set to memorable, weak passwords.

How to reduce the risk

Don't rely on ad-hoc password management: it's too easy for something to slip through. Make sure that the scope of your PAM implementation goes beyond tier 0 accounts to bring all default infrastructure system accounts under proper management.

Listen to
Jean-Christophe Vitu
VP Solution Engineers EMEA:

Assume Breach | Securing Your Infrastructure Accounts

3. LIMIT LATERAL MOVEMENT FROM ENDPOINTS

Think like an attacker

"There's a good chance that senior executives or members of the IT team have local administrative rights to their workstations or that default workstation administrative accounts haven't been touched and are vulnerable to takeover. I'm going to keep at it with phishing emails until I hook someone, then go from there."

How they do it

As long as you have employees with local administrative rights to the machines they are using, attackers will continue to target and exploit them. Even the most IT-savvy user can fall prey to some of today's more sophisticated attack vectors, and many are not particularly IT-savvy.

How to reduce the risk

It's important to educate all your users about security and how to avoid falling prey to attackers. But since there's no way to prevent fallible humans from making mistakes (and mistakes becomes inevitable with enough employees or enough time), you should also, by default, completely remove all endpoint users from the local admin groups on their workstations.

Listen to
Bart Bruijnesteijn
Director Presales
North Europe:

Assume Breach | Limit Lateral Movement

The removal of local administrator rights combined with application control is

100%

effective in preventing ransomware from encrypting files*.

* CyberArk Labs, Analyzing Ransomware and Potential Mitigation Strategies, 2020, https://www.cyberark.com/resources/white-papers/analyzing-ransomware-and-potential-mitigation-strategies-2

4. WIDEN THE PROGRAM AND ACTIVELY MAINTAIN IT

With the first three steps you'll have done the most important work to protect your critical assets, but it won't mean that attackers will stop trying. To further boost your defenses you'll ultimately want to address the many privileged accounts that steps 1, 2 and 3 will leave untouched, namely all of your tier 1 and 2 technical access accounts and application access accounts, including:

- Developer and DevOps accounts
- Business accounts, often shared among multiple users, with privileged access to financial, HR, customer and other systems with sensitive data
- Application access accounts used for any form of system scanning, ticketing, automated login, robotic process automation, or cloud orchestration

Remember, too, that nothing about privileged access management stands still. Infrastructure, applications and employees all come and go, move around, and change in other ways. It takes a structured and continually maintained approach to stay on top of it all, and this should include being able to measure your progress, and regular validation of the effectiveness of your PAM controls against simulated attacks.

Listen to
Christian Götz
Director Presales
DACH:

Assume Breach | Widen the Program

FIND OUT MORE

Visit cyberark.com to learn more about how CyberArk can help you adopt a defense-in-depth approach to security with Privileged Access Management at the core.

About CyberArk

CyberArk (NASDAQ: **CYBR**) is the global leader in Identity Security. Centered on privileged access management, CyberArk provides the most comprehensive security solutions for any identity - human or machine - across business applications, distributed workforces, hybrid cloud workloads, and throughout DevOps pipelines. The world's leading organizations trust Cyberark to help secure their most critical assets. To learn more about CyberArk, visit **www.cyberark.com**.

02.21. Doc. 212302