FIVE WAYS ATTACKERS GET TO DATABASES

NEARLY EVERY ATTACK VECTOR LEADS TO THE DATA.

Below are just a few of the methods attackers use to intrude organizations. Once they are in, they may discover unpatched servers, vulnerable applications and unsecured databases.
The end goal is to exfiltrate, then monetize your sensitive data.

RANSOMWARE

Ransomware, which can be delivered via phishing attacks are increasingly targeting database programs such as MySQL, MongoDB and Hadoop. Ransomware was the largest share of security incidents Trustwave investigated in 2019, which quadrupled over the previous year to encompass 18% of the incidents.
(2020 Trustwave Global Security Report)

MISCONFIGURATIONS

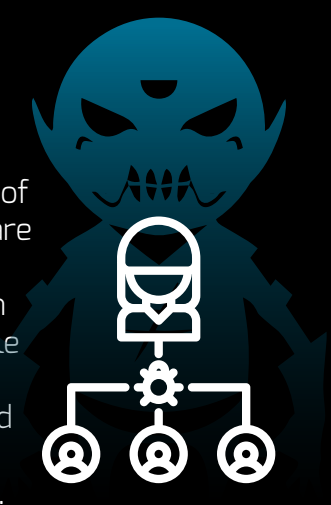
Misconfigured databases have been a major problem across all sectors and makes them vulnerable to attacks. For example, criminals target publicly facing cloud databases using the default settings to compromise its databases and then demand a ransom to release them.
(2020 Trustwave Global Security Report)

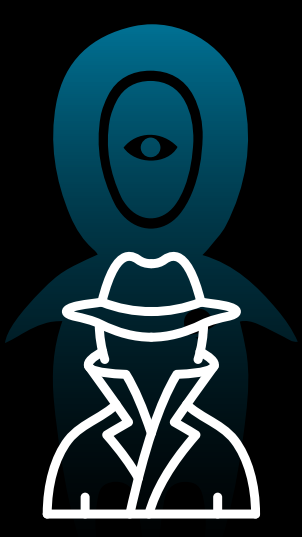
RISE IN VULNERABILITIES

Vulnerabilities are increasing at an unrelenting pace with dire consequences for organizations. For example, in early 2020, Trustwave SpiderLabs researchers discovered six vulnerabilities in SAP Adaptive Server Enterprise (ASE), the most critical of which had a CVSS score of 9.1 (out of 10). Continuously assessing databases for vulnerabilities and continuously monitoring the assets with unapplied patches can help reduce the risk of a data breach.

PRIVILEGE ABUSE

Privilege abuse occurs when the privileges associated with user accounts are operated inappropriately or fraudulently. Privilege escalation involves attackers taking advantage of vulnerabilities in database management software to convert low-level access privileges to high-level access privileges. Privilege escalation requires more effort and knowledge than simple privilege abuse. In the breaches Trustwave investigated in 2019, user credentials accounted for 15% of the cloud data and 18% of the corporate/internal network data compromised.
(2020 Trustwave Global Security Report)





MALICIOUS INSIDER

Insider threats come from people within the organization. For example, Trustwave worked with a client who was experiencing identity theft issues at an increasingly alarming rate. We helped them set up database scanning and monitoring policies using Trustwave DbProtect, our database security and risk management platform. Within a week, Trustwave was able to identify the shrewd thief who was using a known backup time to hide their data siphoning.

THREE DATA SECURITY PITFALLS TO AVOID

CHOOSING TECHNOLOGY FIRST

Work with a partner that has a clear framework for aligning business needs and risks to select a best-fit approach that provides the right level of protection and works well within your current ecosystem.

FOCUS ON REACTING INSTEAD OF BEING PROACTIVE

While rapid threat detection and response is important, it should be paired with a strong vulnerability management program to proactively decrease risks and access to critical data.

LACK OF VISIBILITY

Most solutions in our security ecosystem leave us blind to who is accessing data and how they are using it.

ONE PARTNER WHO CAN HELP YOU DO IT BETTER

Trustwave Database Security Solutions help you get ahead of risks to sensitive data so you can respond intelligently, harden your database attack surface and sustain compliance. Click here for more information.

Trustwave®

www.trustwave.com