Trustwave®

Why a Zero Trust Architecture Must Include Database Security

No matter the mode of cyber-attack – phishing, ransomware, advanced persistent threat, malware, or some combination – the target is generally the same: your data. Your data is valuable to you and your customers, and the bad guys know it.

With traditional network perimeters having essentially evaporated as more and more employees work from home or elsewhere, cyber security professionals struggle to secure networks, applications, devices, people – and data. The trend toward multi-cloud infrastructure only exacerbates the problem, providing more places for valuable data to live.

To protect their data, organizations need to adopt a Zero Trust Architecture approach, based on the principle of "never trust, always verify." **As defined by NIST**, the gist is no person, system, network, or service is trusted, no matter where it's located (within corporate walls vs. the internet) or who owns it. That means you must verify anything and everyone attempting to establish access to your network and/or resources.

Zero Trust, then, also applies to the databases where your valuable crown jewels are stored. In addition to the authorization and authentication that takes place before anyone should be granted access to any of your resources, in a zero trust environment additional measures are needed to ensure the security of your data.

Those measures are required to:

- Identify vulnerabilities in on-premises or cloud databases that attackers could exploit to gain access to your sensitive data
- Limit user access to the most sensitive data
- Alert on suspicious activity, intrusions, and policy violations

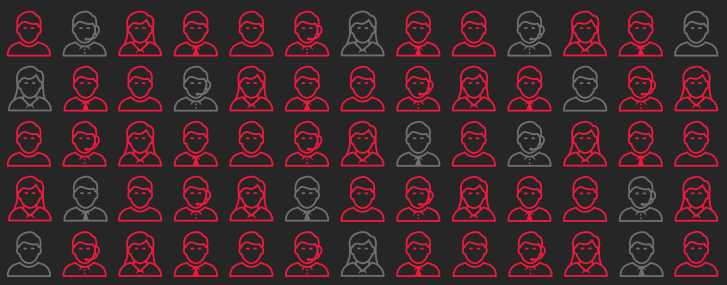
The threat to data is real

The **2022 Verizon Data Breach Investigations Report** contains, as usual, some interesting food for thought on the topic of breaches.

First, 80% of the threat actors in data breaches tend to be external, with only 20% being internal. That aligns with the steady increases we've seen in ransomware in recent years; these folks are truly external bad actors who are out for money, not just internal disgruntled employees or someone who made a mistake.

At the same time, 82% of breaches in the 2022 Verizon report involved "the human element." "Whether it is the use of stolen credentials, phishing, misuse, or simply an error, people continue to play a very large role in incidents and breaches alike," the report said.

The Human Element Dominates in Data Breaches



The human element was involved in 82% of breaches identified in the 2022 Verizon Data Breach Investigations Report, whether the use of stolen credentials, phishing, misuse, or simply an error. Each red symbol represents 25 breaches; n = 4,110.

SOURCE: 2022 VERIZON DATA BREACH INVESTIGATIONS REPORT

So, it seems clear that external actors are preying on (largely) internal employees to ply their trade. That's a powerful combination.

Combatting it requires an equally powerful database security platform that performs in an automated fashion. It needs to be able to ferret out instances of bad actors trying to access your sensitive data, as well as those masquerading as legitimate users, which requires anomaly detection through behavioral models.

Such purpose-built database security provides a number of benefits for any organization:

- Protects your reputation and customer trust
- Saves time while delivering accurate results that instill confidence
- Keeps your name out of the headlines
- Protect your most valuable assets: your data
- Adhere to compliance, regulations, and best practices

Applying Zero Trust to achieve database security

These benefits can be achieved by employing a security software platform specifically designed to address the Zero Trust requirements that databases warrant. Looking for a few key functions will help you ensure the platform is up to the task.

First, it should proactively assess your database security posture to uncover any weaknesses, like vulnerabilities and misconfigurations that can be exploited by attackers and lead to data exfiltration, thus reducing your risk.

Continuous monitoring of database activity is also a must. It should be based on specific policies that you define, so they fit with your organizational security goals. The platform should alert on potential suspicious events based on behavioral models, not just known signatures.

Another function to look for is granular access control and visibility into database accounts with privileged access, whether they're on premises or in the cloud. This allows for the constant validation that only those with a valid purpose have access to administration, application, and service accounts.

Similarly, database security software needs to enforce the principle of least privilege. That means performing deep analysis of the users, roles, objects, and privileges needed to enforce Zero Trust ideals. This enables organizations to limit the database accounts only to those who require access and to enforce data access policies.

Zero Trust and database security resources

To learn more about what goes into a Zero Trust Architecture and how to implement it for your organization, check out the "**Network Security Architecture Assessment and Roadmap**" document from **Trustwave Security Colony**. (A subscription is required for premium Security Colony content, but many resources are free of charge.)

And for more on database security specifically, read our blog post, "**The 10 Principles of Database Security**".

Trustwave®

www.trustwave.com

Copyright © 2023 Trustwave Holdings, Inc.