Oracle Database Insecurity

Hardly a week goes by without at least one announcement of a major IT attack that yielded millions or billions of database records. The target of almost every one of these attacks did what they were told to do. They hired a CISO, installed a firewall, deployed end-point monitoring, wrote a library's worth of documentation on processes and procedures, and passed all of their audits.

If anyone is surprised all of these measures failed... they shouldn't be. Because most of their money, and most of their efforts, had nothing to do with security.

Security Defined

Our failure to secure our data and databases, some of our most valuable Intellectual Property, is the direct result of throwing around a word that we have not defined. Let's do that now.

First, what is *not* security. Security has nothing to do with governance, compliance, audits, auditing, Sarbanes Oxley, HIPAA, PCI, NIST, STIGs, DFARS, or to a great extent Center for Internet Security (CIS).
Security is active measures that prevent unauthorized access, whether internal or external. Security is the actions you take to protect and defend your intellectual property from loss.

This is not to discount the value to an organization when a CISO focuses on passing an audit. Passing audits is an essential function and without compliance the business's ability to operate is put at risk.
But, it is equally essential that the CISO, and the entire technical team whether network, storage, system, or database administrators and developers understand that passing every audit with a 100% score will not prevent a skilled operator from selling your data on the internet 15 minutes later.

The following paragraphs focus on some of the major critical considerations.

Zero Trust Security

Zero Trust is more than just an architecture, it is a state of mind: an approach leads to making better decisions and avoiding the land mines littering the landscape. The point of Zero Trust is that organizations should not trust anything automatically. And by "anything" we mean internal resources, external resources, OEMs, vendors ("vendors" includes consultants). As security consultants we, at Zione, understand that that includes us too. We expect to prove ourselves and to be subject to the same monitoring as everyone else.

A Successful Security Strategy

For a security strategy to be successful it must be both broad and deep. It needs to address all of the threats faced by data and databases, and assign a risk score to each so that organizations can make good decisions for themselves on how to allocate resources in addressing them.

Which is the greater threat to your organization? A backup tape you cannot restore or a GLOGIN attack?
The following categories will help you evaluate whether your security approach will successfully meet your needs.

Data Security

The world is full of threats to your data. Some threats such as ransomware will deny you access. Some threats will alter it. Some threats will exfiltrate it for sale on the internet or to attack additional targets of opportunity.

Depending on the nature of your business, and the data you store, you need to consider all of the following in defining your strategy:

- Backup and Recovery
- Multiple geographically separated data centers, or a hybrid approach using the Cloud
- Data and database archiving

The following listing is an example from an organization now working with Zione this year in which we identified a severe risk to their organization buried inside one of their database's metadata.

```
START_TIME       END_TIME         INPUT_TYPE   STATUS

---------------- ---------------- ------------ ----------------

06/02/2021 00:07  06/02/2021 07:16    DB INCR      FAILED

06/02/2021 10:58  06/02/2021 10:58    ARCHIVELOG   FAILED

06/02/2021 14:58  06/02/2021 14:58    ARCHIVELOG   FAILED

06/02/2021 18:58  06/02/2021 18:58    ARCHIVELOG   FAILED

06/02/2021 22:58  06/02/2021 22:58    ARCHIVELOG   FAILED
06/03/2021 00:07  06/03/2021 00:07    DB INCR      FAILED
```

06/03/2021 02:58	06/03/2021 02:58	ARCHIVELOG	FAILED
06/04/2021 00:07	06/04/2021 07:53	DB INCR	FAILED
06/04/2021 06:58	06/04/2021 08:14	ARCHIVELOG	COMPLETED WITH ERRORS
06/07/2021 06:58	06/07/2021 07:36	ARCHIVELOG	FAILED
06/09/2021 00:07	06/09/2021 06:44	DB INCR	FAILED
06/10/2021 00:07	06/10/2021 08:49	DB INCR	FAILED
06/11/2021 00:07	06/11/2021 10:35	DB INCR	FAILED
06/12/2021 01:00	06/13/2021 23:39	DB INCR	FAILED
06/12/2021 18:58	06/12/2021 19:04	ARCHIVELOG	FAILED
06/15/2021 06:58	06/15/2021 07:25	ARCHIVELOG	FAILED

If there had been a ransomware attack during the first 2 weeks of June they might not have survived.

But backups are not enough. Many organizations encrypt their data, their data at rest, their backups, and exports. If your organization tried to restore a backup from 6 months ago, could you associate that backup with every security certificate and encryption key used in the stack?

When was the last time your organization held a "fire drill" and tried to restore a database from a 30+ day old backup? How would your team perform if you asked them to do it later today?

Data Integrity

One rarely considered aspect of security, because our focus is so often distracted by news stories, is the integrity of our data. The difference between data you cannot rely upon because it has been corrupted by an outside actor, and data you cannot rely upon because of internal processes, is negligible.

Database Configuration: Net Services

The following list, from one of Zione's security customers, is consistent with the configuration of more than 95% of Oracle's customers.

```
LISTENER=(DESCRIPTION=(ADDRESS_LIST=(ADDRESS=(PROTOCOL=IPC)(KEY=LISTENER))))

ENABLE_GLOBAL_DYNAMIC_ENDPOINT_LISTENER_SCAN3=ON

ENABLE_GLOBAL_DYNAMIC_ENDPOINT_LISTENER_SCAN2=ON

ENABLE_GLOBAL_DYNAMIC_ENDPOINT_LISTENER_SCAN1=ON

VALID_NODE_CHECKING_REGISTRATION_LISTENER_SCAN3=OFF    # line added by Agent

VALID_NODE_CHECKING_REGISTRATION_LISTENER_SCAN2=OFF    # line added by Agent

VALID_NODE_CHECKING_REGISTRATION_LISTENER_SCAN1=OFF    # line added by Agent

VALID_NODE_CHECKING_REGISTRATION_LISTENER=SUBNET
```

Valid Node Checking was included in their Enterprise Edition license; it is included in yours too. And Oracle's installation program put the entries into their SQL*Net configuration. The customer just didn't enable it by enabling Valid Node Checking and listing Included Nodes.

Most of Oracle's customers similarly do not mandate a minimum logon version, rate limit connections to prevent a Denial-of-Service attack, or mandate SQL*Net encryption: All of which they already paid for and are included in their Enterprise Edition license.

Database Configuration: Default Profiles and Roles

Oracle's default profiles and roles, upon installation, are by default insecure. Every person or bot wishing to compromise your databases knows that basic configuration. They know that the DEFAULT profile grants unlimited CPU, unlimited I/O. Exactly what they need to not just steal a handful of credit card numbers or passwords but to steal them all. Even the password complexity verification function is in use at fewer than 50% of Oracle's customers and can be enabled in fewer than 5 seconds.

Included Feature

With every Enterprise Edition license comes the ability to enable Row Level Security, which is one of the most powerful ways to prevent unauthorized access. Yet fewer than 5% of Oracle's customers have ever made this capability available to their developers or DBAs.

Proxy Users and Schema Only Accounts

All customers of the Oracle Database are fully licensed to connect using proxy users: Only a small fraction of them

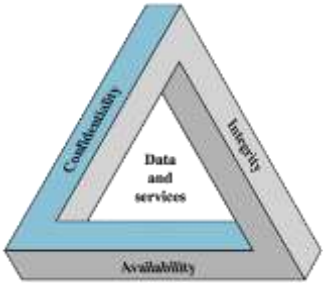
have ever mandated proxy account usage, and yet proxy connections are the most secure connections possible.

With the release of version 18c, Oracle introduced Schema Only Accounts: Accounts that can never be used to log into the database, as a way to secure applications objects and data. Again, only a very small fraction of Oracle's customers, upgrading to 19c and above, have taken advantage of this ability to greatly enhance protection even though the cost of doing so would likely be negligible.

Key Personnel

Fewer than 2% of all Oracle DBAs have received any training on securing an Oracle Database. Some have been trained on deploying products that require additional licensing. They may be able to install Advanced Security, Database Vault, and others, but they have zero training in how to protect against some of the most common configuration issues or prevent a glogin attack.

Wrap Up



We covered a lot of ground in this document, but at a very high level. If database and data security are important to you and to your organization, contact Zione Solutions today and let our security team provide your CISO, your IT management, and your DBAs with a one-hour technical presentation into what we can bring to your organization that will greatly enhance security where it matters: At the database level.