|  |
| --- |
| Home Start Realty |
| Firewall Blocking DB Queries |

To: Brendan McAlister

From: Chad Ballay

During a recent review and audit a security concern was discovered. I wanted to document what we know and the direction we are heading in for resolution.

AS OF NOW WE DO NOT HAVE REASON TO BELIEVE A BREACH HAS OCCURRED, YET.

**Detection**

Two weeks ago while troubleshooting an unrelated issue, I ran the network scanning tool nmap from my personal machine against our network. The results returned showed that our MySQL instance was accessible from the outside network. As part of additional detection efforts I ran the same test from additional machines both internal and external. At this we confirmed that the firewall was not blocking incoming our outcoming traffic for our database.

**Analysis**

* Enabled query monitoring to identify if data was being infiltrated or exfiltrated. This will only tell us what is occurring from this point forward.
* Connections will still need to authenticate with valid credentials.
* Reviewed our existing logging to see if we could identify if adversaries had previous to our monitoring been engaged. (We do not have the data to rule this out.)
* Reviewed that data we maintained to see if we had any that related to PCI, SOX, CCPA, or other legally protected data. (We do not have confirmation of a breach so this was to scope the potential size of impact.)
* Reviewed the firewall to see if this had been disabled or ever been in place to protect the database from external/internal access. (We do not have confirmation that this had ever blocked database traffic and the outside world.)

**Containment**

At this point we are continuing to log the connections to look for any suspicious activities. We do not have confirmation of a breach. We also do not have any information pointing to this being malfeasance.

**Recommendation**

I strongly recommend we block all direct access to the database by updating the firewall. There is no business justification that matches industry standards to allow this to remain. Several arguments can be made to this greatly increasing our risk to data loss, breach, or other negative consequences.

As a follow on step I also advise we rotate the passwords for all accounts for the database immediately after the firewall step is done.

A regular scheduled scan of our network, both internal and external, should be done. The frequency will need to be researched but a continuous scan and alerting procedures would provide us with immediate confirmation.

Research into the feasibility of implementing Honey Tokens within the database records as well as various Honeypot-as-a-Service solutions should be undertaken.

Finally, this has shown that if we were to have a breach we do not have the logging and monitoring in place to identify access attempts from unsanctioned sources. A review of our monitoring posture should be undertaken to identify what should we now put in place if this were to occur again.

Once this in place a formalized escalation policy should be created for identifying processes and procedures on managing any future similar situations. This lack of a process increased our MTTR. Adopting the NIST CyberSecurity Incident Response guidelines would be a good starting point.