The unfortunate cybersecurity risks quantum computers pose to SA businesses

By Riaan de Villiers

25 Mar 2021

The big difference between current (traditional) computers and quantum computers is that quantum computers could process information much faster. Processing that will take traditional computers years to perform could theoretically be completed by a quantum computer in a matter of hours.

Photo by Anna Shvets from Pexels

Cybercriminals make their living by attacking businesses and people around the world. Technologies such as quantum computers can create an opportunity for cybercriminals to execute even more catastrophic cyberattacks.

Fortunately, Public Key Infrastructure (PKI) can secure organisations. As long as cybercriminals do not know what your keys - encryption and/or decryption - are, your data is safe. However, quantum computing can change that.

Brute-force attack

For example, in cybersecurity, there is a cyberattack called a brute-force attack, where attackers can try to guess your key. By checking every possible value, the attacker would be able to guess your key eventually. However, with the current technology, to guess all possibilities for keys would take hundreds of years, which makes brute-force attacks impractical.

Since quantum computers will be much faster, they can, theoretically, guess an encryption and/or decryption key in a matter of hours.

7 steps to keep your SME cyber safe

24 Mar 2021

There is still much speculation about what the post-quantum world would be like, but organisations can start preparing for when the inevitable comes.

Even though readily available quantum computers are still in the distant future, organisations can start thinking about their strategy to become more crypto agile. To prepare for the world of quantum computing, organisations can:

- Create a crypto inventory. A list of cryptographic algorithms in use will help organisations identify vulnerable algorithms and migrate them to quantum-resistant algorithms when it becomes necessary.
- Start building your systems with crypto agility in mind. For example, when applying digital signatures use PAdES (PDF Advanced Electronic Signatures) compliant standards that will allow you to re-timestamp your documents with quantum-resistant algorithms.
- Ask your third-party platform providers what they are doing to prepare for the post-quantum world.

ABOUT THE AUTHOR

Riaan de Villiers is a cybersecurity expert and business analyst at LAWTrust.