Preparation for Post-Quantum Security

Student

Linda Graber

Introduction: Quantum computers, once the stuff of science fiction, are on the verge of becoming reality. Thanks to billions in investment from governments and private parties, great progress has been made in recent years. Quantum computers have the ability to change the world by helping to tackle climate change, invent new drugs or improve large language models used in AI. But great opportunities also come with risks: quantum computers will be able to break the encryption methods that are widely used today. Future quantum computers are already threatening encrypted data today; in so-called "harvest now, decrypt later" attacks, encrypted data is stolen today with the aim of decrypting it as soon as the technology is available.

Approach: The aim of this paper is to understand how great the risk of the so-called quantum threat is and what can be done to minimize the former. The first step was to develop a basic understanding of the technology and the current state of research. With this knowledge, the research phase began, which was divided into two parts. The first part involved reading assessments of the situation by national security agencies. The assessments of these security experts made it possible to evaluate the urgency of this threat. In the second phase, various migration recommendations from different institutions were analyzed. This made it possible to put together a suitable strategy for Vontobel in the final phase of the project.

Result: The analysis of the white papers of the security agencies drew a very clear picture, all papers recognized the potential threat posed by a quantum computer. Today's encryption standards will not be able to withstand a quantum computer. Encrypted data is already at risk today as it is harvested to be decrypted at a later date. A new encryption standard is expected to be introduced at the beginning of 2024. To prepare for this and implement the new standards as early as possible, it is recommended to plan for a migration in advance. Several agencies have issued a recommendation for action. The migration papers differ somewhat in terms of content, but agree on many points. These suggestions were used to summarize a suitable strategy for tackling the migration at Vontobel. The resulting migration plan consists of the following main points: creating awareness of the threat and educating employees at all levels, creating an inventory of the existing infrastructure and data stock, using the gathered information to create a risk assessment that outlines measures for each infrastructure component and create a timeline when which components will be migrated to achieve a quantum safe state.

Advisor
Dr. Alexandru Caracas

Subject Area
Computer Science