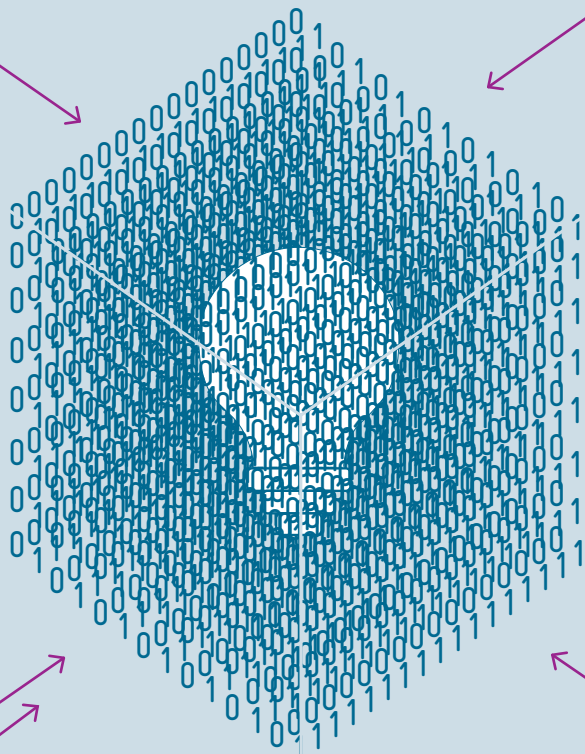


B 2 Cybersicherheit

Die fortschreitende Digitalisierung und digitale Vernetzung bieten neue Angriffspunkte auf Unternehmen. Innovationsaktivitäten von Unternehmen sind von dieser Gefahr direkt betroffen.

Schadprogramme führen unerwünschte oder schadhafte Funktionen auf einem Computersystem aus.

Mit Ransomware verschlüsselt ein Angreifer die Daten eines IT-Systems, um die Nutzerinnen und Nutzer dazu zu bewegen, ein Lösegeld zu zahlen.



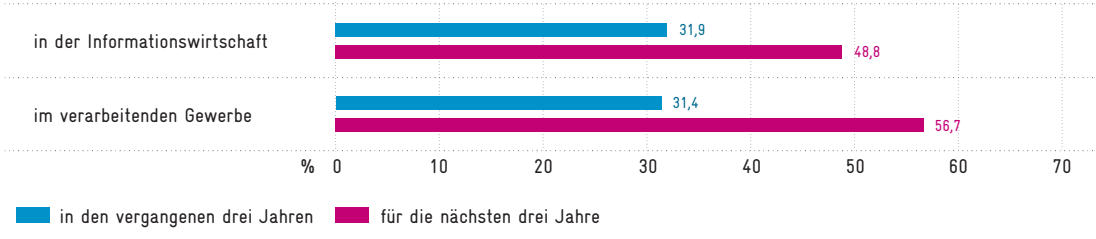
Advanced Persistent Threats weisen ein hohes Bedrohungspotenzial auf, weil die Angreifer gezielt und ausdauernd Schwachstellen ausfindig machen, um sie dann auszunutzen.

Durch Social Engineering werden Personen manipuliert, um sie dazu zu bringen, vertrauliche Informationen preiszugeben, Dateien oder Links mit hinterlegten Schadprogrammen zu öffnen oder Geld an unberechtigte Empfänger zu überweisen.

Bei DDoS-Angriffen fallen Netzwerkdienste aus, nachdem sie durch eine Vielzahl von Anfragen überlastet und somit blockiert wurden.

Einschätzung von Unternehmen zur Entwicklung der Gefahr durch Cyberangriffe¹⁾

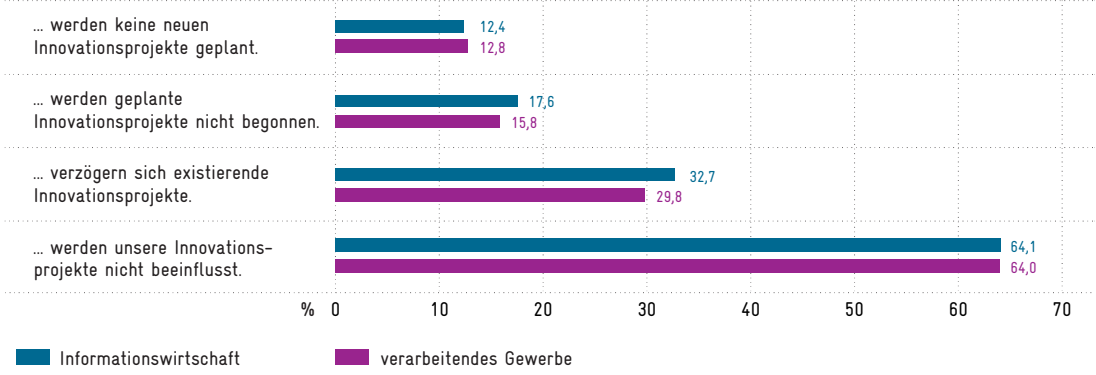
Anstieg oder starker Anstieg der Gefahr durch Cyberangriffe ...



Branchenspezifische Hochrechnung der Ergebnisse auf die Frage: „Wie schätzen Sie die Veränderung der Gefährdung durch Cyberangriffe für Ihr Unternehmen ein?“. Lesebeispiel: 56,7 Prozent der Unternehmen des verarbeitenden Gewerbes erwarten einen Anstieg oder starken Anstieg der Gefährdung durch Cyberangriffe für die nächsten drei Jahre.

Auswirkungen von Cyberbedrohungen auf Innovationsaktivitäten²⁾

Durch die Gefahr eines Cyberangriffs ...



Branchenspezifische Hochrechnung der Ergebnisse auf die Frage: „Welche Auswirkungen hat die Gefahr eines Cyberangriffs auf die Innovationstätigkeit Ihres Unternehmens?“. Mehrfachnennungen möglich. Lesebeispiel: 12,8 Prozent der Unternehmen des verarbeitenden Gewerbes planen wegen der Gefahr eines Cyberangriffs keine neuen Innovationsprojekte.