



ANGREIFER IM VISIER

Cyber Defence Maturity Assessment nimmt
Angriffsmethoden und Schutzmaßnahmen
unter die Lupe

Ob Script-Kiddies, finanziell motivierte Cyber-Kriminelle oder politisch motivierte Akteure: Unternehmen werden heutzutage von sehr unterschiedlichen Angreifern attackiert – und jede Angreifergruppe arbeitet mit ihren Methoden.

Um den immer ausgefeilteren Angriffen zu begegnen, müssen Unternehmen diese Angriffstechniken kennen und sich auf diese vorbereiten. Nur so können sie Gefahren abwehren, Vorfälle erkennen und adäquat darauf reagieren. In der Praxis können dies aber nur die wenigsten.

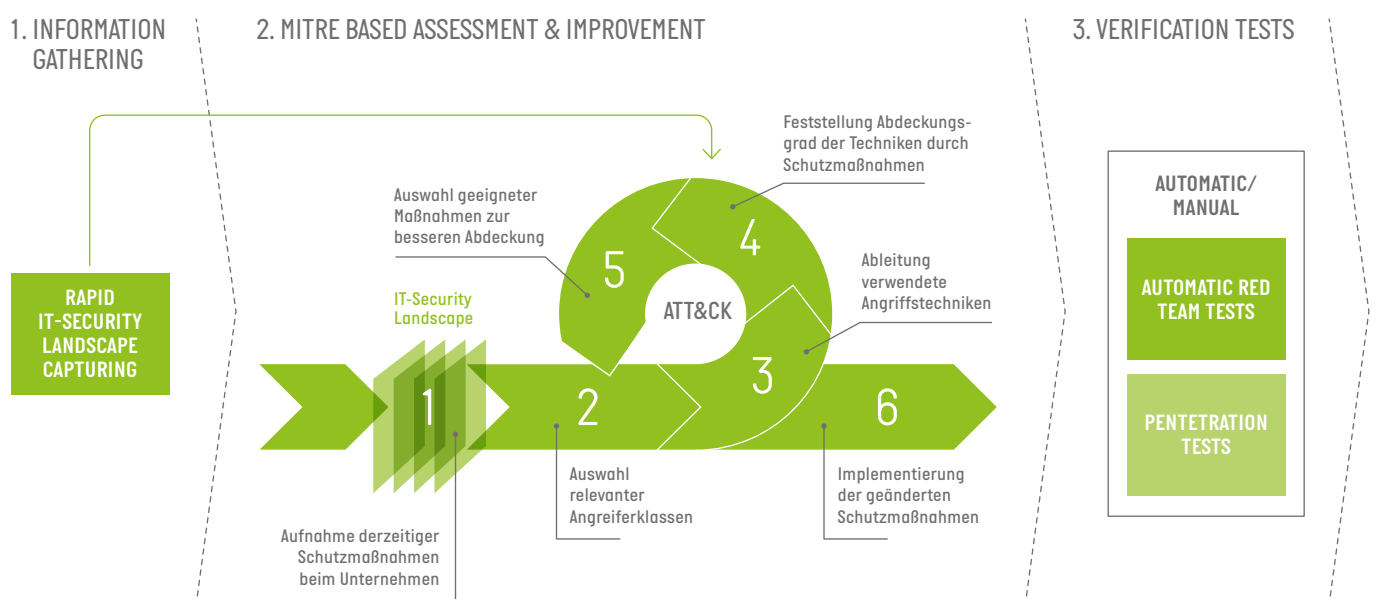
Weil viele Unternehmen gar nicht wissen, gegen welche Angriffsmethoden sie sich schützen müssen und ob ihre existierenden Maßnahmen überhaupt wirksam sind, können sie weder ihr Sicherheitslevel einschätzen noch die richtigen Maßnahmen zur Verbesserung ihres Schutzniveaus umsetzen.

Mit dem Computacenter ‚Cyber Defence Maturity Assessment‘ lässt sich schnell Klarheit schaffen. Im Rahmen des Assessments geben wir Ihnen Antworten auf Fragen wie:

- Welche Angreifer haben Interesse an meinem Unternehmen?
- Welche Angriffstechniken verwenden diese Angreifer?
- Wie gut verhindern bzw. erkennen meine Schutzmaßnahmen diese Techniken?
- Welche Angriffstechniken erkennen meine Schutzmaßnahmen nicht?
- Welche meiner Schutzmaßnahmen sind inzwischen obsolet?
- Wie lassen sich Lücken sinnvoll schließen?

ERKENNTNISREICH: GEGENÜBERSTELLUNG VON ANGRIFFSTECHNIKEN UND SCHUTZMASSNAHMEN

Dazu haben wir eine Methodik entwickelt, um die Widerstandsfähigkeit von IT-Infrastrukturen zu bewerten. Basis hierfür ist die stets aktuelle MITRE ATT&CK™-Wissensdatenbank, die alle bekannten Angriffstechniken, Angriffsvektoren und typischen Angreiferklassen anhand der Phasen einer Cyber-Attacke zusammenführt. Mit unserem Cyber Defence Maturity Assessment bewerten wir anhand von etwa 230 MITRE-Angriffstechniken individuell für Sie, wie wirksam Ihre bestehenden Schutzmaßnahmen gegen diese sind. Konkret betrachten wir Maßnahmen für Prävention & Detektion sowie die Response-Fähigkeiten Ihres Unternehmens gegenüber den unterschiedlich motivierten und technisch versierten Angreiferklassen.



WIE GEHEN WIR VOR?

Unsere Methodik unterteilt sich in drei Phasen: Erfassung des Status Quo, Bewertung auf Basis von MITRE ATT&CK sowie Verifikationstests.

In der ersten Phase „Erfassung des Status Quo“ erfassen wir die in ihrem Unternehmen verwendeten technischen Sicherheitsmaßnahmen mittels einer Schnellaufnahme, so dass innerhalb kurzer Zeit alle notwendigen Informationen zusammengeführt werden – auch für internationale, große Unternehmen mit vielen Standorten.

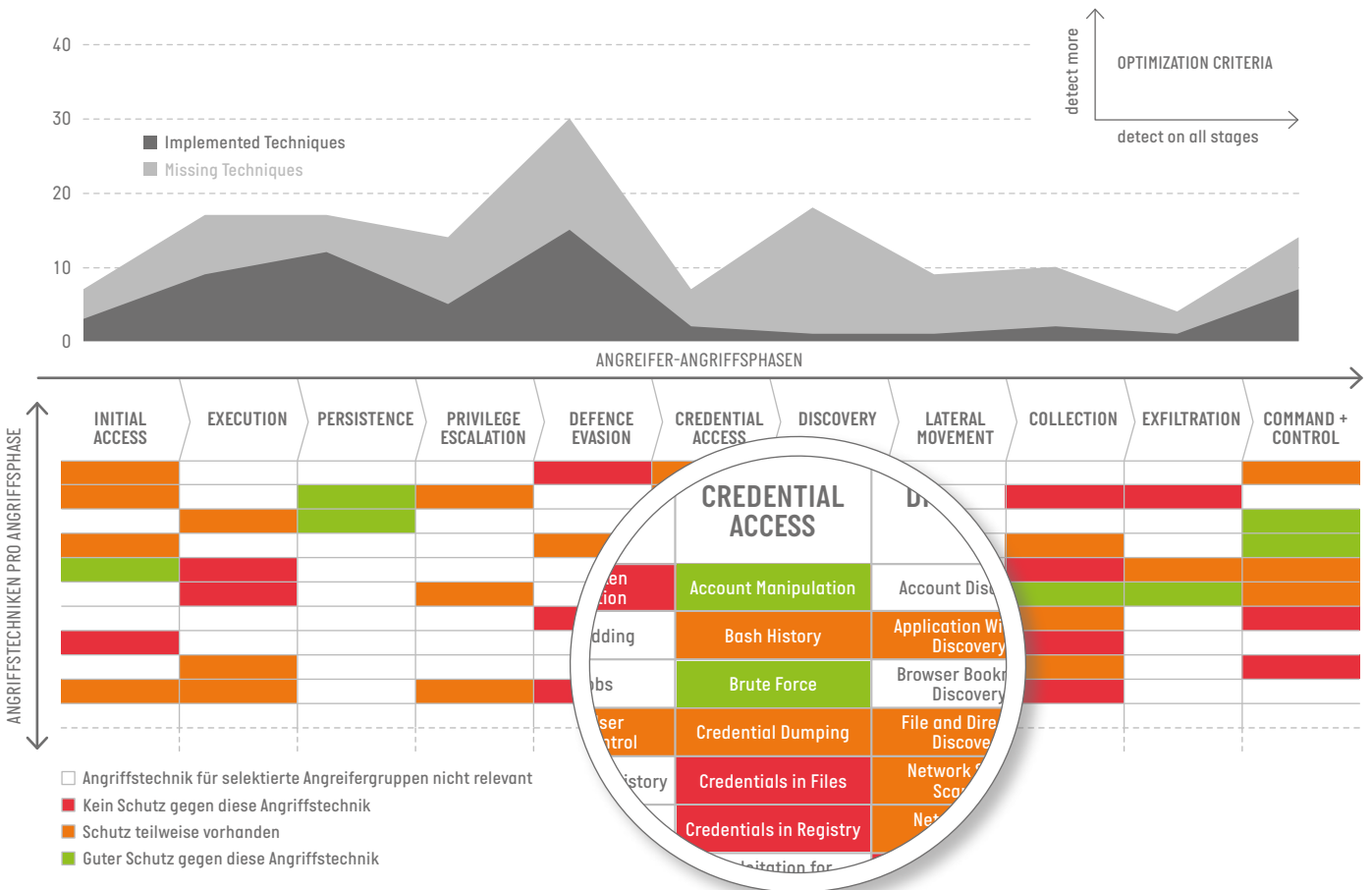
In der zweiten Phase erfolgt die eigentliche Bewertung. Hierfür gehen wir in sechs Schritten vor:

1. Definition relevanter Angreiferklassen
2. Ableiten der Angriffstechniken, gegen die ein Schutz gewährleistet sein muss
3. Feststellen des Abdeckungsgrades gegen diese Techniken durch die bestehenden Schutzmaßnahmen [Welche Technik wird wie gut abgedeckt?]
4. Vorschlag geeigneter Schutzmaßnahmen für eine bessere Abdeckung

In der dritten Phase, der Verifikation, können die Sicherheitsmaßnahmen eines Unternehmens gegen Angriffstechniken getestet werden. Die Tests konzentrieren sich auf die Angriffstechniken, deren Abdeckung beim Assessment aufgrund fehlender Informationen nicht zu 100 Prozent zugesichert werden können oder welche inzwischen nachgebessert wurden.

WO GREIFEN DIE BESTEHENDEN SCHUTZMASSNAHMEN? WELCHE ANGRIFFS-TECHNIKEN WERDEN GUT, TEILWEISE ODER GARNICHT ABGEDECKT?

Unser Cyber Defence Maturity Assessment gibt Auskunft, wo Angreifer leichtes Spiel haben und nachgebessert werden sollte.



FUNDIERTE ENTSCHEIDUNGSGRUNDLAGE FÜR INVESTITIONEN

Mit dieser Vorgehensweise arbeiten wir systematisch die Schutzdefizite Ihrer IT heraus. Sie erhalten ein klares Bild davon, wo Ihre IT gut geschützt ist und wo Lücken zu schließen sind. Zusätzlich ist ein Vergleich der abgedeckten Angriffstechniken mit anderen Organisationen im gleichen Industriesegment

möglich. Gleichzeitig erhalten Sie konkrete Empfehlungen, wie Sie Ihr Sicherheitslevel wirtschaftlich und effizient erhöhen können. So bietet unser Cyber Defence Maturity Assessment nicht nur eine realistische Einschätzung Ihres Schutzniveaus, sondern auch eine fundierte und nachvollziehbare Entscheidungsgrundlage für Investitionen in die IT-Sicherheit.

Unternehmensprofil

Computacenter ist der führende, unabhängige Anbieter von IT-Infrastrukturservices und -lösungen für Großunternehmen und große Organisationen des öffentlichen Sektors. Wir unterstützen unsere Kunden bei der Beschaffung, Transformation und Verwaltung ihrer IT-Infrastruktur und bei der Umsetzung ihrer digitalen Transformation.

Computacenter ist eine Aktiengesellschaft, die im Londoner FTSE 250 Index notiert ist und weltweit rund 15.000 Mitarbeiter beschäftigt.