Was ist ein «Digital Immune System»?

Dominic Beusch, Wirtschaftsinformatiker, exec. MBA in Digital Transformation

In einer Welt, die zunehmend von digitalen Technologien geprägt ist, wird der Schutz digitaler Systeme und Daten zu einer der grössten Herausforderungen für Unternehmen und Organisationen. Ob es sich um persönliche Informationen, Finanztransaktionen oder geschäftskritische Daten handelt, die Gefahr von Cyberangriffen ist allgegenwärtig. Um dieser ständigen Bedrohung zu begegnen, spielt das Konzept des «Digitalen Immunsystems» eine entscheidende Rolle. Dieser Artikel erläutert das digitale Immunsystem und beleuchtet anhand konkreter Beispiele, wie es dazu beiträgt, digitale Umgebungen vor Bedrohungen zu schützen.

Ein digitales Immunsystem umfasst eine Vielzahl von Sicherheitsmassnahmen und -technologien, die digitale Systeme vor Bedrohungen schützen. Es ist vergleichbar mit dem menschlichen Immunsystem, das den Körper vor Infektionen schützt. Nachfolgend sind einige Schlüsselelemente eines digitalen Immunsystems aufgeführt:

- **Firewalls und Intrusion-Detection-Systeme (IDS)**: Firewalls überwachen den Datenverkehr zwischen einem internen Netzwerk und dem Internet, während IDS verdächtige Aktivitäten erkennen. Ein gutes Beispiel sind Firewalls und IDS-Systeme, die in Unternehmen zum Schutz sensibler Finanzdaten eingesetzt werden.
- **Zugangskontrollen und Berechtigungen**: Durch die Definition von Berechtigungen und Zugriffsbeschränkungen können Systemadministratoren den Zugriff auf bestimmte Applikationen und Daten in digitalen Systemen einschränken. Beispiel: Ein Mitarbeiter hat nur Zugriff auf die Daten, die er für seine Arbeit benötigt.
- **Security Information and Event Management (SIEM):** SIEM-Systeme sammeln, analysieren und korrelieren Sicherheitsinformationen und Ereignisprotokolle, um Bedrohungen zu erkennen und darauf zu reagieren. Beispiel: Prüfung der Protokolle nach verdächtigen Aktivitäten, um einen Angriff zu identifizieren und nötigenfalls abzuwehren.
- **Sicherheitsschulung und Sensibilisierung**: Schulung und Sensibilisierung der Benutzer sind entscheidend, um sicherzustellen, dass sie sich der potenziellen Gefahren und sicherheitsbewussten Praktiken bewusst sind. Beispiel: Schulungen, in denen die Mitarbeitenden ermutigt werden, auf verdächtige E-Mails zu achten und keine sensiblen Informationen preiszugeben.
- **Incident Response und Krisenmanagement**: Ein Plan für den Umgang mit Sicherheitsvorfällen, der sicherstellt, dass Bedrohungen schnell erkannt und eingedämmt werden. Beispiel: Ein gut vorbereitetes Krisenmanagement-Team, das sofort auf einen Sicherheitsvorfall reagiert.
- **Disaster Recovery und Backup-Strategien**: Planung für den Fall eines schwerwiegenden Sicherheitsvorfalls, um Systeme bei einem Katastrophenfall

wiederherstellen zu können. Beispiel: Regelmässige Backups und Wiederherstellungspläne zur Vermeidung von Datenverlusten.

- **Machine-Learning-basierte Bedrohungserkennung**: Viele Unternehmen nutzen Machine Learning und künstliche Intelligenz, um Bedrohungen in Echtzeit zu erkennen. Diese Systeme analysieren riesige Datenmengen und identifizieren ungewöhnliche Aktivitäten, die auf potenzielle Angriffe hinweisen.
- **Zero-Trust-Security-Modelle**: Zero Trust ist ein Sicherheitskonzept, das nicht vertrauenswürdige Netzwerke oder Benutzer blockiert. Jeder Benutzer und jedes Gerät muss sich bei jedem Zugriffsversuch authentifizieren und der Zugriff wird auf ein Minimum beschränkt.

Reale Beispiele für ein digitales Immunsystem

Die folgenden Beispiele aus der Praxis zeigen, wie das digitale Immunsystem digitale Umgebungen vor Bedrohungen schützen kann.

Swisscom (2018): Die Swisscom, der grösste Telekommunikationsanbieter der Schweiz, war Ziel eines Angriffs, bei dem die persönlichen Daten von rund 800.000 Kunden gefährdet waren. Dieser Angriff zeigte die Notwendigkeit für Schweizer Unternehmen, ihre Sicherheitsmassnahmen zu verstärken und ihre digitalen Immunsysteme zu optimieren.

Schweizer Regierung (2022): DDoS (Distributed Denial of Service) ist ein Cyberangriff, der versucht, eine Website durch Überfluten mit schädlichem Traffic zu überlasten, sodass sie nicht mehr betrieben werden kann. Ein solcher DDoS-Angriff erfolgte auf die Website der Schweizer Regierung und führte zu einer vorübergehenden Unterbrechung der Site. Der Angriff wurde durch den Einsatz von DDoS-Schutzdiensten abgewehrt.

SBB (2023): Einen Cyberangriff gab es ebenfalls bei der SBB im Februar 2023. Cyberkriminelle haben Schadsoftware über E-Mails verbreitet. Dabei ist es den Angreifern gelungen, in einen Teil des Unternehmensnetzwerks der SBB einzudringen. Die SBB haben den Cyberangriff analysiert und die Sicherheitsmassnahmen erhöht.

Key Takeaway

Ein digitales Immunsystem ist unerlässlich, um digitale Systeme und Daten vor den ständig wachsenden Bedrohungen (Phishing, Malware, DDoS etc.) zu schützen. Es besteht aus einer Vielzahl von Sicherheitsmassnahmen und -technologien, die einen Schutzwall um digitale Lebensräume bilden. Die hier aufgeführten Massnahmen zeigen, wie diese Sicherheitsmassnahmen in der Praxis funktionieren und wie sie dazu beitragen, digitale Umgebungen sicherer zu machen. In einer Zeit, in der die Abhängigkeit von der digitalen Welt laufend zunimmt, ist ein starkes digitales Immunsystem unerlässlich, um Daten und Privatsphäre zu schützen.