DCSO
Engineering Security.
Together.

SECURITY TECHNOLOGY

7 Schritte zur fundierten Produktauswahl

DCSO Deutsche Cyber-Sicherheitsorganisation GmbH
EUREF-Campus 22
10829 Berlin, Germany
info@dcso.de
+49 (0) 30 726219-0
www.dcso.de

Intro

Durch die Bank investieren Unternehmen immer größere Beträge in IT-Security und zugehörige Produkte. Dennoch sind Nachrichten über Datendiebstahl, kompromittierte Umgebungen und erfolgreiche Ransomeware an der Tagesordnung.

Entweder IT-Security-Produkte funktionieren generell nicht (und eine ganze Industrie verkauft im wesentlichen Schlangenöl) oder Firmen kaufen die falschen Produkte, um sich effektiv zu schützen. Branchenunabhängig zeigen sich bei der Auswahl von IT-Sicherheitsprodukten dabei immer wieder Muster, die darauf hindeuten, dass viele Unternehmen konsequent Fehlentscheidungen bei der Produktauswahl treffen.

Dieses Whitepaper zeigt eine fundierte Herangehensweise an die Auswahl von IT-Security-Produkten und beleuchtet die Mechanismen, die hinter den Fehlentscheidungen stehen – damit Sie sie umgehen können.

Aufmerksamkeitsökonomie

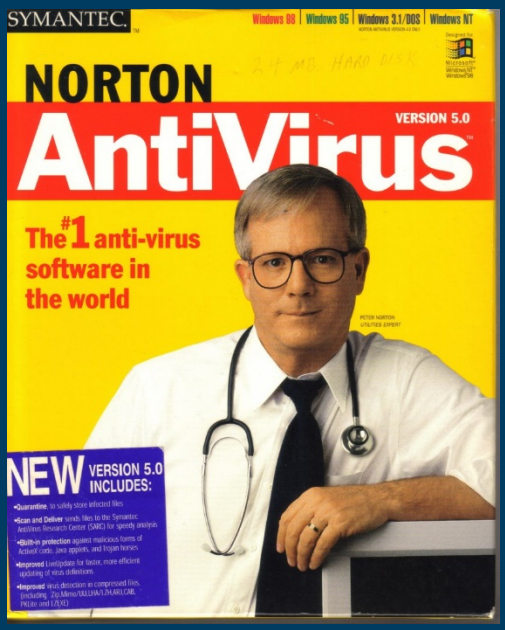
Der Vertrieb von IT-Security-Produkten hat sich in den letzten Jahren gewandelt. Beispielhaft lässt sich dieses gut an zeitgenössischem Marketing illustrieren.

Bild 1 zeigt eine Werbung für Norton Antivirus 5 aus den 1990er Jahren[1]. Die neuen Features der Version 5 sind unter anderem ein Schutz vor bösartigen Java Applets und Erkennung von Viren auch in komprimierten Formaten wie ZIP, ARJ und Mime/UU (ähnlich zum heutigen Base64).

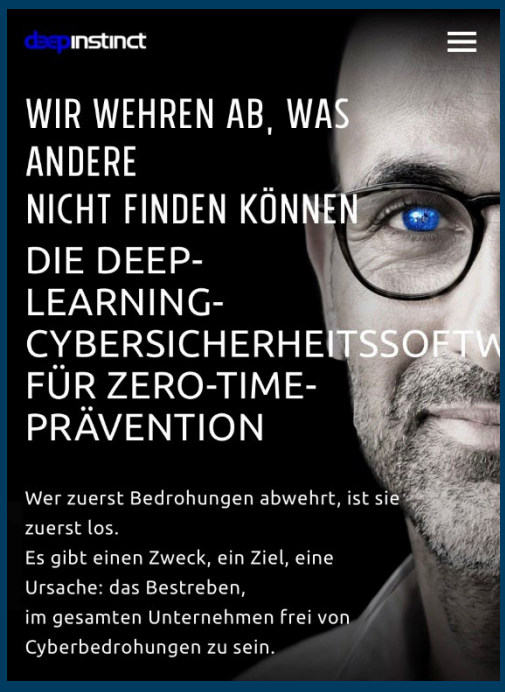
Das zweite Bild zeigt einen Screenshot der Webseite von Deep Instinct, einem Anbieter von deep-learning gestützten AV Produkten[2]. Der Hersteller wirbt mit "Die Deep-Learning-Cybersicherheitssoftware für Zero-Time-Prävention".

Beide Produkte verfolgen das gleiche Ziel: Den Computer des Anwenders vor Schadsoftware zu schützen. Dennoch sind die Ansprachen unterschiedlich: Die Norton- Werbung aus den 1990er Jahren adressierte klar ein technisches Publikum. Die Zielgruppe waren Anwender, die Abkürzungen wie "PKLite", "Mime/UU", "ActiveX Code" nicht abschreckend fanden, sondern sie als positives Funktionsmerkmal wahrnehmen.

Deep Instinct verspricht denselben Nutzen, adressiert aber sichtbar ein anderes Publikum. Anstatt technischer Begriffe ist die Ansprache managementorientiert. "Es gibt einen Zweck, ein Ziel, eine Ursache: das Bestreben, im gesamten Unternehmen frei von Cyberbedrohungen zu sein", heißt es.



Norton Werbung



Deep Instinct Homepage

[1] https://hampdencomputer.com/2014/09/antivirus-expired-playing-with-fire/

[2] https://www.deepinstinct.com/de/

Die Ansprache adressiert nicht primär Techniker, sondern richtet sich an Entscheider. Die Fokussierung des Vertriebs auf Personen im Management ist ein genereller Trend.

Hersteller würden diese Form der Ansprache nicht wählen, wenn sie nicht funktionieren würde. Dahinter verbirgt sich einer der Gründe, aus dem Unternehmen konsequent unpassende Sicherheitsprodukte einkaufen: Das Setzen eines geschickten Triggers innerhalb der Kundenorganisation.

Guter Trigger, schlechter Trigger?

Jede Produktauswahl beginnt mit einem Trigger. Auswahlprozesse, die aus den falschen Gründen gestartet wurden, führen zu unbefriedigenden Ergebnissen. Oft ist es einfacher den Auslöser an sich zu hinterfragen, als den Prozess später zu stoppen. Daher ist es sinnvoll, möglichst früh zu überdenken, warum überhaupt ein Produkt ausgewählt werden soll.

Unserer Erfahrung nach führen einige Trigger notorisch zu fragwürdigen Produkt-entscheidungen:

Das Middle- oder Upper-Management wurde durch einen persönlichen Kontakt auf eine Lösung aufmerksam
Aus operativer Sicht wird das Produkt nicht benötigt, dennoch wird der Hersteller zu einem Termin geladen um den Vorschlag angemessen zu behandeln.

Der Vertrieb des Produktanbieters lädt sich selbst zu einer Produkt-vorstellung ein
Meist bringen diese nur einen sehr begrenzten Erkenntnisgewinn. Jedes Produkt sieht (wenn es ansprech-end präsentiert wird) für sich genommen sinnvoll aus. Ansprechende Präsentationen korrelieren allerdings nicht unbedingt mit tauglichen Produkten.

Diese Trigger haben gemein, aus Sicht der Fachabteilung ex-trinsisch zu sein. Es steht kein nachvollziehbarer Bedarf hinter der Produktauswahl, sondern sozialer Druck.

Die richtigen Trigger

Natürlich ist nicht jede Produktauswahl zum Scheitern verurteilt. Es gibt sinnvolle Gründe ein bestehendes Produkt abzulösen oder bestehende Fähigkeiten durch eine neue Lösung zu erweitern. Diese Trigger sind intrinsisch. Aus Sicht der Fachabteilung basieren intrinsische Motivationen üblicherweise auf einem technischen Bedarf, sie können aber z.B. auch finanziell sein.

Beispiele für diese Trigger sind:

1. Vertrag endet

Die Laufzeit eines Produktvertrages endet und es öffnet sich ein Fenster, um die bestehende Auswahl zu hinterfragen.

2. Einführung einer neuen Architektur

Aus einer neuen Architektur oder einem Konzept ergeben sich neue Angriffsvektoren, die abgesichert werden müssen. Beispiele: eine Migration zu Office 365, macOS Endpoints oder BYOD.

3. Schwachstellen werden bekannt

Durch Penetration-Testing, Reviews der bestehenden Konzepte oder neue Compliance-Anforderungen ergeben sich Schwachstellen im bestehenden Portfolio.

Aus der Praxis

Ein DCSO-Kunde betreibt derzeit eine alleinstehende EDR-Lösung parallel zu einer bestehenden Microsoft Defender for Endpoint Installation. Im Rahmenvertrag des Kunden sind Microsoft Defender ATP-Lizenzen vorhanden.

Da der Vertrag mit dem EDR-Anbieter ausläuft, erhofft sich der Kunde durch eine Konsolidierung der Fähigkeiten in der Microsoft Plattform sowohl finanzielle als auch operative Vorteile. In diesem Zuge möchte der Kunde auch Systeme in der Azure Cloud, die bislang nicht über einen EDR-Agenten überwacht wurden, anbinden. Daher führt der Kunde eine Evaluation durch, um sicherzustellen, dass Microsoft Defender ATP die internen Anforderungen erfüllt.

7 Schritte zum richtigen Produkt

Im Folgenden stellen wir einen Prozess vor, der in sieben Schritten zu einer belastbaren und nachvollziehbaren Produktauswahl führt. Als Expert:innen für Security Technology bei der DCSO führen wir seit Jahren Tests nach diesem Schema erfolgreich durch.

1. Use Cases

Jeder Produkttest sollte mit Anforderungen starten, die als Use Cases dokumentiert werden. Auch wenn das nach einer Plattitüde klingt, vernachlässigen viele Unternehmen diesen Schritt sträflich. In der Realität beginnt man oft schon an Tag 1 der Evaluation das Gespräch mit dem Hersteller und recherchiert nach Produkten. Doch diese "Effizienzmaßnahme" versperrt den Blick fürs Wesentliche – den realen Anforderungen des Unternehmens. Zeit, die in solide Use Cases investiert wird, zahlt sich am Ende doppelt aus: In der Argumentation der Entscheidung genauso wie in der Implementierung der Lösung. Wir empfehlen die Use Cases in funktionale und nicht-funktionale Anforderungen aufzuteilen:

Funktionale Use Cases

Sie bilden den Grund ab, weshalb ein Produkt eingesetzt wird. Bei einer EDR-Lösung also Sichtbarkeit zu Events auf dem Endpoint oder bei einem SIEM die Anbindung diverser Datenquellen aus dem Unternehmen.

Nicht-funktionale Use Cases

Diese "Hygienekriterien", sind Kriterien, die ein Produkt erfüllen muss. Beispielhaft sind hier eine vernünftige Dokumentation, benutzbares User Interface und angemessene Skalierbarkeit zu nennen.

Aus der Praxis

In der praktischen Anwendung bricht unser Team die übergreifenden Use Cases in kleinere Test Cases auf. Jeder Test umfasst dabei 200 bis 400 einzelne Cases, die granular bewertet werden können. Zur Verwaltung nutzen wir TestRail der deutschen Firma Gurock. Das Tool stammt aus der Qualitätssicherung, funktioniert für unsere Anforderungen aber gut. Für kleinere Projekte lässt sich sicherlich auch ein Excel-Sheet nutzen.

Unserer Erfahrung nach werden nicht-funktionale Use Cases bei Proof of Concepts (PoCs) in Unternehmen häufig vernachlässigt. Auch namenhafte Tests reflektieren oft nur die funktionalen Kriterien.

Die Erfüllung von nicht-funktionalen Anforderungen ist in der Realität aber immens wichtig. Eine EDR-Lösung mit schlechtem Interface wird schlicht nicht gut funktionieren. Wir kennen Fälle, in denen viel Geld in EDR-Lösungen investiert wurde, die wegen Compliance-Bedenken durch den Betriebsrat aussortiert wurden.

Die fehlende Einbeziehung nicht-funktionaler Kriterien ist einer der Knackpunkte, warum Unternehmen trotz einer gewissenhaften Auswahl unpassende Produkte kaufen. Auf die Frage, warum diese Kriterien bislang vernachlässigt wurden, sind die Antworten vielfältig. Immer wieder wird genannt, dass diese Kriterien...

... nicht so gut messbar wären und eine subjektive Bewertung nicht gewünscht ist

... in der Zielgruppe nicht als relevant eingeschätzt werden oder nicht bekannt ist, welche Kriterien erfüllt werden müssen

Um Konflikte im Ablauf zu vermeiden, muss die Dokumentation multi-user-fähig sein (in der Praxis also Excel-Online). Tools aus der Qualitätssicherung sind erstaunlich günstig und bieten hilfreiche Features, wie automatische Auswertungen, die den Preis rechtfertigen.

2. Verantwortlichkeiten und Stakeholder

Eine ordentliche Evaluation ist praktisch nicht als Nebenaufgabe im Tagesgeschäft durchzuführen. Für Security-Produkte fällt diese Aufgabe oft Administratoren und Analysten zu, die sowieso schon priorisieren müssen. Allzu häufig fällt die Tiefe eines Tests anderen Rollen zum Opfer. Wir empfehlen daher, eine Evaluation als eigenständiges Projekt zu betrachten.

Produktauswahl als Projekt

Es sollte also ein Projekt-Management haben und über ein Team, Kapazitäten und Budget verfügen. Wenn diese Basics nicht zugesagt werden können, ist es meist besser, die Evaluation zu verschieben oder outzusourcen. Unserer Erfahrung nach genügen für die tiefgehende Beschäftigung mit einer Lösung inklusive Installation drei bis vier Personenwochen. Der Aufwand hängt aber natürlich von der Zahl der zu testenden Use Cases ab.

Die Betrachtung als Projekt bringt mit sich, dass projektrelevante Stakeholder identifiziert werden müssen. Diese können Teil der Evaluation sein (wie das IT-Betriebsteam) aber auch spätere Nutzer der Lösung. Idealerweise nehmen alle Stakeholder die Use Cases zur Kenntnis, bevor die Evaluation startet. Wenn es einen Betriebsrat gibt, sollte auch er schon in dieser frühen Phase eingebunden werden. Erfahrungsgemäß entscheiden Betriebsräte eher vorsichtig und je früher sie am Prozess teilnehmen, umso mehr Verständnis haben Sie für das Gesamtprojekt.

Unser Tipp

Das IT-Betriebsteam kann in einem informellen Gespräch meistens gut einschätzen, wie lange die Installation der Lösung braucht. Je früher die Kolleg:innen einbezogen werden, umso glatter läuft der Start in den PoC. Meistens lohnt sich hier der direkte Dienstweg, um bei den Beteiligten ein Team-gefühl (und damit eine wahrgenommene Verant-wortung) herzustellen.

3. Marktbetrachtung

Aus dem Dschungel der Produkte die richtigen für eine Evaluation zu finden, ist nicht einfach. Insbesondere wenn der spätere Test nicht komfortabel mit Zeit und Ressourcen gesegnet ist, ist die Vorauswahl schon essenzieller Teil der Evaluation. Auch wenn es verführerisch ist, nur die Produkte zu betrachten, die bei gängigen Analysten Erwähnung finden, führt dieser Ansatz nicht zu optimalen Ergebnissen.

Unser Tipp

Fragen, die sowieso von jedem Hersteller gleich beantwortet werden ("Kann ihr Produkt DSGVO-konform betrieben werden?"), sind es nicht wert im Fragebogen aufzutauchen, da sie keinen Mehrwert für die Evaluation bieten.
Wenn das Produkt sich nicht DSGVO-konform einsetzen lässt, wäre der Vertrieb in Deutschland schließlich nicht zulässig. Eine bessere Frage ist "Wurde unabhängig geprüft, wie sich Ihr Produkt DSGVO-konform einsetzen lässt? Wenn ja, von wem?"

Stattdessen lohnt es sich einen kurzen Fragebogen zu erstellen, der die primären Einsatzzwecke der gesuchten Lösung beschreibt. Der Fragebogen muss die Use Cases nicht in der Tiefe abbilden, es genügen zehn bis 15 präzise Fragestellungen, an denen sich die Lösung messen muss.

Nach dem Fragebogen lohnt es sich, interessante Produkte auch im Rahmen einer Demonstration kennen zu lernen – am besten geführt durch einen Engineer des Herstellers. Inzwischen trauen es sich die wenigsten Hersteller aus so einem Termin eine Folienschlacht zu machen. Sollte es doch einmal zu marketing-lastig werden, genügt oft ein kurzer Hinweis auf das praktische Interesse. Schlussendlich hat auch der Hersteller ein Interesse möglichst schnell über das konkrete Produkt und seine Anwendung zu sprechen.

Während der Demonstration zahlen sich dokumentierte und präzise Use Cases als Leitfaden aus. Aus dem Fragebogen und den Ergebnissen der Herstellerdemos ergeben sich so zwei bis fünf vielversprechende Produkte, die in den weiteren Schritten näher betrachtet werden.

4. Proof of Concept: Vorbereitung

Wenn noch nicht geschehen, sollten als erster Schritt des PoC die abstrakten Use Cases in konkrete Test Cases umgewandelt werden. Test Cases müssen dokumentieren, welche Funktionalität gewünscht ist und wie diese geprüft werden kann. Zeit, die in die Vorbereitung investiert wird, zahlt sich eigentlich immer aus, wenn man sie mit Ad-hoc-Aufgaben während eines laufenden PoC vergleicht.

Wie in allen Schritten gilt: Eine saubere Dokumentation ist der Schlüssel, um effizient testen zu können.

Wie bereits erwähnt, sind insbesondere nicht-funktionale Test Cases ein außerordentlich wichtiger Testbestandteil. In der Praxis scheitern viele Produkteinführungen an nicht-funktionalen Problemen. Es lohnt sich also, einen Plan zu machen, welche Aspekte der Dokumentation, Integration mit Bestandslösungen und des Lifecycles geprüft werden sollen.

Neben den organisatorischen Vorbereitungen müssen auch die technischen Vorbereitungen für den PoC getroffen werden. Die genaue technische Vorbereitung hängt natürlich vom Produkt ab. Zu empfehlen sind isolierte Testumgebungen, um die Komplexität niedrig zu halten und Fehlerquellen zu vermeiden.

Es gilt mit Augenmaß zu agieren:

Welche Komponenten müssen im PoC angebunden werden?

Muss das produktive SIEM verbunden werden oder genügt eine kleinere Testinstallation?

Unser Tipp

Hersteller von Security-Produkten bieten Bestands-kunden oft kostenlos eine zeitlich begrenzte Testlizenz des genutzten Produktes an. Diese Lizenzen eignen sich gut für den Einsatz als Integrationstest, ohne dass die produktive Instanz des Produktes angebunden werden muss.

Natürlich sollte jede Integration mit produktiven Systemen dokumentiert werden, um sie nach dem Rückbau des PoC zurückbauen zu können. Nach der Vorbereitung der Test Cases und Infrastruktur können die zu evaluierenden Produkte ausgerollt werden. Vor der Installation empfehlen wir den Zeitrahmen des Tests mit dem Hersteller konkret abzustecken. Ein Test ohne Zeitdruck klingt verlockend, resultiert in der Realität aber in nie endenden Zyklen von Produktpatches und Konfigurationsanpassungen. Unserer Ansicht nach genügen drei Wochen intensives Testen, um genug Einblick in die Leistungsfähigkeit eines Produktes zu bekommen.

5. Durchführung des Tests

In den meisten Tests, die wir durchführen, bietet der Hersteller an, das Produkt selbständig zu installieren und integrieren. Auch wenn es attraktiv erscheint, so gleich zu Beginn des Tests Aufwand zu sparen, empfehlen wir dieses Vorgehen nicht. Aus unserer Sicht ist die Installation bereits Teil des Tests und bietet viele Einblicke in das Produktdesign, Dokumentation und Reife.

Selbst installieren ist von Vorteil

Wir empfehlen daher das Produkt selbst zu installieren, gerne mit Unterstützung des Herstellers. Eine eigene Installation erlaubt es einzuschätzen wie komplex das Produkt ist und welche Fallstricke im Betrieb lauern. Sollte der Hersteller keine eigene Installation des Produktes erlauben, weil diese zu komplex oder zu schlecht dokumentiert ist, überlegen wir ernsthaft, ob ein weiterer Test sinnvoll ist.

Was für die Installation gilt, gilt auch für die Konfiguration

Der Hersteller kann mit Erfahrungswerten und Empfehlungen unterstützen, doch die Konfiguration sollte selbständig vorgenommen werden. Während der meisten PoCs sind Änderungen an der Konfiguration ohnehin notwendig, zudem ist die initiale Konfiguration eine her- vorragende Möglichkeit diese kennenzulernen.

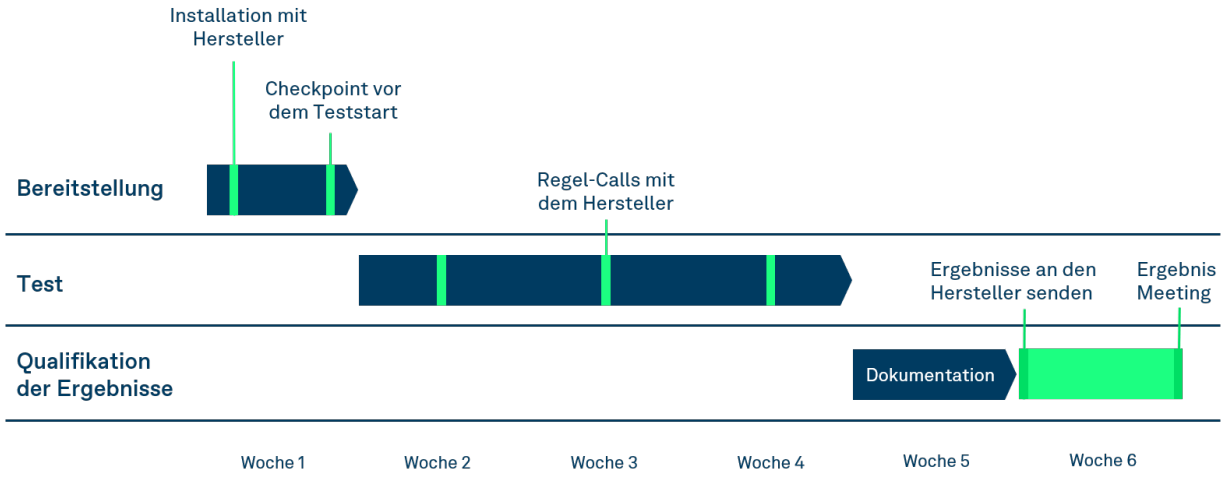
Was ist mit SaaS?

Bei Produkten die als SaaS betrieben werden, findet natürlich keine klassische Installation des Backends statt. Dennoch muss in den meisten Fällen etwas lokal installiert werden: Agenten auf Endpunkten, Gateways um interne Systeme zu erreichen oder Plugins zur Integration.

Während des Tests gilt es, Kontakt zum Hersteller zu halten. Dennoch sollte der Hersteller bei der eigentlichen Ausführung der Tests nicht präsent sein, denn er wird natürlich versuchen, die Ergebnisse in seinem Sinne zu beeinflussen. Anstatt einer dauerhaften Anwesenheit empfehlen wir regelmäßige Touchpoints, um Fragen und Probleme zu diskutieren.

Ein sauber durchgeführter Test wird zwangsläufig Schwachstellen und Probleme identifizieren. Wir empfehlen diese dem Hersteller zu kommunizieren und einen Behebungsplan einzufordern. Wenn dieser in die Entscheidung einfließen soll, muss er allerdings konkret vereinbart sein und die Erfüllung geprüft werden. Die Erfahrung zeigt, dass man sich auf vage Ideen und mündliche Versprechungen nicht verlassen kann.

Das folgende Bild zeigt eine Struktur für die Herstellerkommunikation, die sich bei uns in den letzten Jahren bewährt hat. Bei akuten Problemen kann der Hersteller aber immer angesprochen werden, um die Zeitplanung nicht zu gefährden.



6. Ergebnisdokumentation

Wir empfehlen die Ergebnisse wie folgt zu trennen, damit während der Entscheidung Fakten von Eindrücken getrennt behandelt werden.

Fakten

Alle Test Case-Ergebnisse sollten mit einer kurzen Begründung und Beschreibung gebündelt werden. Hier hat sich eine Skala von 0 (nicht implementiert, fehlt) bis 3 (besser als notwendig) bewährt. Eine Gewichtung kann helfen klarzustellen, welche Anforderungen den größten Einfluss haben.

Eindrücke

Das zweite Dokument enthält alle Informationen, die sich nicht tabellarisch abbilden lassen:
Eindrücke während des Tests, der Installation und Konfiguration sowie Beschreibungen der Testumgebung.

7. Entscheidung

Der beschriebene Prozess wurde über Jahre zusammen mit Kunden entwickelt und erfolgreich in Projekten eingesetzt. Das Vorgehen führt natürlich nur zum Erfolg, wenn die Dokumentation auch in der finalen Entscheidung berücksichtigt wird. Die Behandlung als Evaluationsprojekt soll auch dazu führen, dass auf Management-ebene die Ergebnisse ernst genommen werden und die Entscheidung maßgeblich beeinflussen.

Die perfekte Auswahl benötigt also zwei Dinge:

1. **Aufmerksamkeit auf Ebene der Entscheider**
2. **Eine Dokumentation, welche diese Aufmerksamkeit auch verdient**

Takeaways

Um teure Fehlinvestitionen zu vermeiden, sollte vorab genau geprüft werden, ob Bestandsprodukte die geforderten Fähigkeiten abbilden können.

Sollte eine Investition notwendig sein, empfehlen wir die Produktentscheidung als Projekt zu begreifen, das basierend auf strukturierten Kriterien zu einer belastbaren Bewertung führt.

Diese Kriterien sollten nichtfunktionale Anforderungen wie Dokumentation, Useability, Compliance und Betriebsstabilität mit umfassen. Auch der Preis einer Lösung kann als Kriterium aufgefasst werden.

Die praktische Evaluation sollte mehrere Produkte umfassen und sich eng an die definierten Kriterien halten.

Anstatt einer permanenten Überwachung durch den Hersteller empfehlen wir einen unabhängigen Test mit regelmäßigen Touchpoints.

Eine strukturierte Ergebnisdokumentation stellt sicher, dass die Testergebnisse bei der finalen Produktentscheidung angemessen berücksichtigt werden.

Über Security Technology Services der DCSO

Die Security Technology Services der DCSO identifizieren und evaluieren herstellerneutral vielversprechende IT-Sicherheitslösungen und unterstützen Unternehmen dabei, in einem dynamischen und sich ständig verändernden Markt die Nase vorn zu haben.

Die Deutsche Cyber-Sicherheitsorganisation wurde 2015 durch die Gesellschafter Allianz SE, BASF SE, Bayer AG und Volkswagen AG gegründet – als Antwort auf die asymmetrische Bedrohung durch global agierende, organisierte Cyberkriminalität und staatlich gelenkte Wirtschaftsspionage. Die DCSO bringt Unternehmen, Behörden und Institutionen zusammen und gestaltet vertrauensvollen Austausch untereinander. Darauf aufbauend entwickelt die DCSO State-of-the-Art-Services zur effektiven und effizienten Abwehr, von denen alle Mitglieder profitieren.

DCSO Deutsche Cyber-Sicherheitsorganisation GmbH
EUREF-Campus 22
10829 Berlin
+49 30 72 62 19 0
dcso.de