IT-SECURITY

Den Bock zum Gärtner machen:
Warum der IT-Betrieb von IT-Sicherheits-Experten überwacht werden sollte

„Den Bock zum Gärtner machen“ bedeutet, jemandem eine Aufgabe zu übertragen, für die er offensichtlich ungeeignet ist."

Quelle: Duden – Deutsches Universalwörterbuch

Der IT-Betrieb ist für viele Unternehmen eine Herausforderung. Aus diesem Grund bedienen sie sich Systemhäusern und IT-Service Dienstleistern, die den Betrieb für sie übernehmen. Und diese Beziehung hält dann meist schon seit vielen Jahren.
Mit der zunehmenden Komplexität bekam in der Vergangenheit auch die Frage größere Bedeutung, wer nun die Absicherung der IT für die auftraggebenden Unternehmen übernehmen würde. Allzu naheliegend war in dieser Frage die Entscheidung, die beauftragten IT-Dienstleister mit dieser wichtigen Aufgabe zusätzlich zu belegen.
Und heute steht man vor der Frage, ob hier nicht der Bock zum Gärtner gemacht wurde, ohne aber, dass dieser das eigentlich jemals sein wollte.

Und dann die neuen Herausforderungen!

Heute zeigt uns die Praxis hier eine neue Seite der Komplexität! Die Herausforderungen für die beauftragenden Unternehmen selbst wurde spätestens mit der EU-DSGVO und zuletzt auch im Besonderen mit der NIS2 klar erkennbar. Denn die Unternehmen sind nun auch dafür verantwortlich, dass ihre Dienstleister die Compliance-Anforderungen erfüllen und sämtliche Vorkehrungen getroffen haben, um Hackerangriffe effektiv zu verhindern.
Aber wie sollen die beauftragenden Unternehmen das bewerkstelligen?
Sie haben ja nicht einmal die Klarheit darüber, dass ihre IT-Dienstleister alle Maßgaben erfüllen, eventuelle Hackerangriffe auf die unternehmenseigene IT zu verhindern. Klar, die Dienstleister sind gehalten, ihren Auftraggebern die Überwachung der gemanagten IT mittels Reporting und Audits zu belegen. Aber diese Informationsbasis reicht hier nicht aus, um die wesentlichen zwei Fragen vollständig zu belegen:

1.) Ist das eigene Unternehmen mit seiner IT compliant und ausreichend geschützt?
2.) Ist der Auftragnehmer mit wiederum seiner eigenen IT compliant und ausreichend geschützt?

Für das beauftragende Unternehmen besteht also das Problem, dass es sich damit auseinander muss, was eigentlich im Betrieb wie abgesichert sein sollte. Zudem müssen sie die Compliance-Berichte zur Einhaltung verstehen oder überhaupt lesen, was den IT-Dienstleister in eine vollkommen unkontrollierte Position bringt. All dies kann zu Problemen führen, die sich in folgenden Punkten manifestieren.

Die Probleme einer fehlenden externen IT-Security-Kontrolle

Wenn der IT-Dienstleister, der das System entwickelt und betreibt, auch für deren Security-Überwachung verantwortlich ist, entsteht ein potenzieller Interessenkonflikt. Folgende Probleme können auftreten:

- **Mangelnde Objektivität:** Der IT-Dienstleister hat grundsätzlich wenig Interesse daran, eigene Fehler, nicht geschlossene Schwachstellen oder sogar sicherheitsrelevante Vorfälle offenzulegen, da dies seinen Ruf schädigen und zu Schadensersatzzahlungen führen könnte.
- **Fehlende Transparenz:** Ohne externe Kontrolle gibt es keine unabhängige Instanz, die prüft, ob Sicherheitslücken bestehen oder ob Compliance-Richtlinien eingehalten werden.
- **Eingeschränkte Expertise:** IT-Betrieb und IT-Security sind zwei unterschiedliche Fachgebiete. Ein IT-Dienstleister, der sich primär auf Betrieb konzentriert, verfügt oft nicht über das tiefgehende Wissen zu den neuesten Bedrohungen und Abwehrmechanismen.
- **Fehlende Kontrolle über privilegierte Zugänge:** Wenn der IT-Dienstleister selbst die Zugänge verwaltet, besteht das Risiko, dass sensible Daten oder administrative Rechte missbraucht werden.
- **Schlechte Reaktionsfähigkeit:** Ohne eine dedizierte Security-Instanz werden Sicherheitsprobleme oft erst bemerkt, wenn es bereits zu spät ist.
- **Fehlende Compliance-Überwachung:** Der Dienstleister übernimmt die Überwachung im Auftrag des Unternehmens, das eigentlich für die Einhaltung des Dienstleisters verantwortlich ist.

Aber wie kommt man als beauftragendes Unternehmen aus der Bredouille heraus, wenn es aus eigener Kraft die Überwachung bewerkstelligen kann?
Man beauftragt einen weiteren IT-Security-Dienstleister, der den IT-Betrieb-Dienstleister operativ und dauerhaft überwacht und zumindest die wichtigsten Kontrollaufgaben übernimmt, um bestmöglichen Schutz zu übernehmen. Eine auditierende Aufgabenstellung, also die punktuelle und bewertende Überprüfung der Kontrollmechanismen durch Dritte reicht hier nicht aus.

Wie ein spezialisierter IT-Security-Dienstleister für Sicherheit sorgt

Ein externer Security-Dienstleister kann diese Probleme durch spezifische Sicherheitsmaßnahmen effektiv angehen. Besonders wichtig sind hierbei unter anderem:

1. **Schwachstellenmanagement**
   Ein Security-Dienstleister führt kontinuierliche Schwachstellenanalysen durch und

identifiziert potenzielle Angriffsflächen, bevor diese ausgenutzt werden können. Zu den Maßnahmen zählen:

- Regelmäßige Sicherheits-Scans zur Identifikation von Schwachstellen.
- Patch-Management zur Behebung von Sicherheitslücken in Betriebssystemen und Anwendungen.

2. **Privileged Access Management (PAM)**
   Privilegierte Konten sind eines der größten Sicherheitsrisiken in Unternehmen. Ein IT-Dienstleister hat oft weitreichende Berechtigungen, die im Missbrauchsfall schwerwiegende Folgen haben können. Ein Security-Dienstleister sorgt durch PAM für eine strenge Kontrolle dieser Zugänge:
   - Just-in-Time-Zugriffe: Administrative Berechtigungen werden nur für die Dauer einer bestimmten Aufgabe vergeben und danach entzogen.
   - Session-Monitoring: Administrator-Aktionen werden in Echtzeit überwacht und protokolliert.
   - Multi-Faktor-Authentifizierung (MFA) für sensible Zugriffe.

3. **Strikte Firewall-Regeln und Netzwerksegmentierung**
   Eine unzureichend konfigurierte Firewall oder fehlende Netzwerksegmentierung kann Angreifern ermöglichen, sich im System auszubreiten. Ein externer Security-Dienstleister stellt sicher, dass:
   - Minimalprinzips-Ansatz (Least Privilege) umgesetzt wird, sodass nur notwendige Verbindungen erlaubt sind.
   - Regelmäßige Firewall-Audits stattfinden, um unautorisierte Änderungen zu erkennen.
   - Netzwerksegmentierung eingesetzt wird, um kritische Systeme von weniger sensiblen Bereichen zu trennen.

Aber welcher Dienstleister kann als IT-Security-Dienstleister fungieren?

Wählt das beauftragende Unternehmen einen IT-Security-Dienstleister aus, der selbst auch den IT-Betrieb anbietet, entsteht unweigerlich eine Konfliktsituation, da der IT-Betriebsdienstleister befürchten könnte, dass ihm Aufgaben durch den überwachenden Security-Dienstleister streitig gemacht werden.. Eine notwendige Kooperationsbereitschaft unter den beiden Dienstleistern kann daher kaum gewährleistet sein.
Der zu wählende IT-Security-Dienstleister darf daher nur Dienstleistungen im Bereich der IT-Security anbieten, da er so keine Gefahr für den beauftragten IT-Betrieb-Dienstleister darstellt. Mehr noch, mit der Hinzunahme des IT-Security-Dienstleister entfällt für den IT-Betrieb-Dienstleister die Nachweispflicht der Einhaltung der Compliance, die für ihn weitaus aufwändiger ist, als diese durch den überwachenden Dienstleister nachweisen zu lassen.

Mehrkosten durch die Beauftragung eines zweiten Dienstleisters kaum zu erwarten!

Für das beauftragende Unternehmen entstehen durch die Beauftragung zweier Dienstleister kaum Mehrkosten, da der überwachende Dienstleister Tätigkeiten übernimmt, die ansonsten dem IT-Betrieb-Dienstleister ohnehin übertragen werden müssen.
Durch die Spezialisierung und die hohe Effizienz des IT-Security-Dienstleister kann dieser zudem die übertragenden Aufgaben meist günstiger anbieten als der IT-Betrieb-Dienstleister, bei welchem oftmals Know-how und Ressourcen in den Überwachungsaufgaben knapp sind.
Im Gegenzug erhält das beauftragende Unternehmen eine deutlich größere Transparenz über die Einhaltung der Sicherheitsüberwachung. Es kann sich selbst im Rahmen des Nachweises der Einhaltung von Compliance-Anforderungen deutlich besser entlasten, da die Dokumentation nun vollständig an den IT-Security-Dienstleister übergeht.

Fazit: Will man also den Gärtner zum Gärtner machen?

Die Frage, die man sich als beauftragendes Unternehmen stellen muss, ist die Abwägung zwischen Vertrauen und effizienter Kontrolle des IT-Betriebsdienstleisters im Thema der Sicherheit des bereitgestellten IT-Betriebs. Egal, wie groß das Vertrauen ist, wenn es um Sicherheit geht, ist es wichtig, dass der eine Managed Service dem anderen Managed Service über die Schulter schaut. Denn wenn einer nur sich selbst kontrolliert, besteht immer die Gefahr, dass Schwachstellen übersehen werden – ungeachtet ob durch mangelnde Expertise, fehlende Kapazität oder Verlust der Objektivität.
Will ein Unternehmen, die durch Compliance-Normen aufgezwungene Verantwortung über seine Dienstleister übernehmen und dabei seinen IT-Betrieb effektiv schützen, geht das nur durch die Hinzunahme eines IT-Security-Dienstleisters.