CISO READ

How & Why

cybovate

Sicherheitsstrategie

Mehr tun bedeutet nicht unbedingt mehr Sicherheit:

Fokus auf das Wesentliche

Inhalte

Fokus auf das Wesentliche

Die Ablenkung

Im heutigen Cybersecurity-Markt werden kleine und mittelständische Unternehmen mit Tools, Checklisten, Frameworks und gut gemeinten Ratschlägen regelrecht bombardiert. Von Compliance-Checkboxen bis hin zu Endpoint-Detection-Lösungen, von Phishing-Simulationen bis zu Threat-Intelligence-Feeds – der Druck, „alles zu machen“, ist enorm.

Doch die Wahrheit ist: Mehr tun bedeutet nicht unbedingt mehr Sicherheit. Tatsächlich kann der Versuch, alles abzudecken, zu blinden Flecken, Überforderung, falsch konfigurierten Tools und verschwendeter Zeit führen. Viele Profis unterschätzen die Komplexität des Themas Cybersecurity. Die Idee dieses Whitepepers ist, einen Ausweg aufzuzeigen: nicht, indem man alles macht, sondern indem man die wichtigsten Dinge richtig macht.

Tool-Müdigkeit und die Illusion von Sicherheit

Viele kleine Unternehmen tappen in die Falle zu glauben, dass mehr Tools auch mehr Schutz bedeuten. Die Realität ist jedoch, dass das Aneinanderreihen von Tools ohne klare Strategie oft zu Doppelarbeit, Fehlalarmen, ignorierten Warnmeldungen und Lücken zwischen den Lösungen führt.
Noch schlimmer: Viele Tools erfordern umfangreiche Konfiguration und laufende Wartung, für die kleine Teams weder Zeit noch das nötige Fachwissen haben.
Sicherheit wird nicht an der Anzahl von Dashboards gemessen. Sie wird an Ergebnissen gemessen – daran, ob Angreifer in Ihre Umgebung eindringen, sich festsetzen und ausbreiten können. Mehr Tools hinzuzufügen kann diese Ergebnisse verschleiern, anstatt sie zu verbessern.

Es ist an der Zeit, Cybersicherheit nicht mehr nur anhand der Zahl der Findings oder nach dem Budget zu messen.
Es ist an der Zeit, den Schwerpunkt auf Klarheit und Kontrolle zu legen.

KMU-Realität: Begrenzte Zeit, begrenztes Budget

Die meisten kleinen Organisationen verfügen nicht über ein eigenes Sicherheitsteam. Manche haben nur eine Person, die mehrere Rollen gleichzeitig ausfüllt. In diesem Umfeld zählt jede Stunde. Die Frage sollte nicht lauten: „Was können wir noch zusätzlich tun?“, sondern: „Was macht uns tatsächlich sicherer?“.

Sicherheit sollte das Geschäft unterstützen, nicht blockieren. Wenn eine neue Maßnahme zu viel Reibung oder Wartungsaufwand verursacht, wird sie zur Belastung. Schlimmer noch: Sie kann zu schlechtem Verhalten oder zur Umgehung führen.

Einfachheit ist für kleine und mittelständische Unternehmen kein Luxus, sondern eine Überlebensstrategie.

Start, Stop, Simplify: Ein Framework für mehr Klarheit

Anstatt endlos weitere Tools hinzuzufügen, nutzen Sie den Ansatz **Start / Stop / Simplify**, um im Bereich Sicherheit den Focus auf das Wesentliche zu bekommen.

Start

- Beginnen Sie damit, Ihre Sicherheitslage aus Sicht eines Angreifers zu bewerten. Denken Sie in Ergebnissen, nicht in Checklisten.
- Fangen Sie mit grundlegenden, wirkungsvollen Maßnahmen an: MFA, Backups, Phishing-Schutz, Patchen ausnutzbarer Schwachstellen.
- Entwickeln Sie einen einfachen, wiederholbaren Prozess, um zu testen, was funktioniert.

Stop

- Hören Sie auf, jedem neuen Tool oder Schlagwort ohne klaren Anwendungsfall hinterherzujagen.
- Verlassen Sie sich nicht ausschließlich auf Compliance-Frameworks als Nachweis für Ihre Sicherheit.
- Gehen Sie nicht davon aus, dass mehr Warnmeldungen gleichbedeutend mit mehr Schutz sind.

Simplify

- Vereinfachen Sie, indem Sie sich überschneidende Tools zusammenführen.
- Vereinfachen Sie das Reporting, um sich auf konkrete und tatsächliche Risiken zu konzentrieren.
- Vereinfachen Sie das Onboarding, die Schulungen und den täglichen Betrieb.

Das sollte Ihnen helfen, den Lärm zu reduzieren und sich auf das zu konzentrieren, was wirklich zählt – und so das heute bestehende Risiko zu verringern.

Tatsächliches vs. Gefühltes Risiko: Ein anderer Ansatz

Nicht alle Bedrohungen sind gleich. KMUs müssen wie Angreifer denken: Was würden sie ausnutzen? Was ist exponiert? Welcher Weg führt wirklich zu einem Schaden?
Das gefühlte Risiko wird von Schlagzeilen und dem Marketing der Anbieter bestimmt. Das tatsächliche Risiko basiert darauf, ob Ihre Verteidigungsmaßnahmen umgangen oder Schwachstellen ausgenutzt werden können. Priorisieren Sie die Maßnahmen, die die Wahrscheinlichkeit und die Auswirkungen tatsächlicher Angriffe verringern.

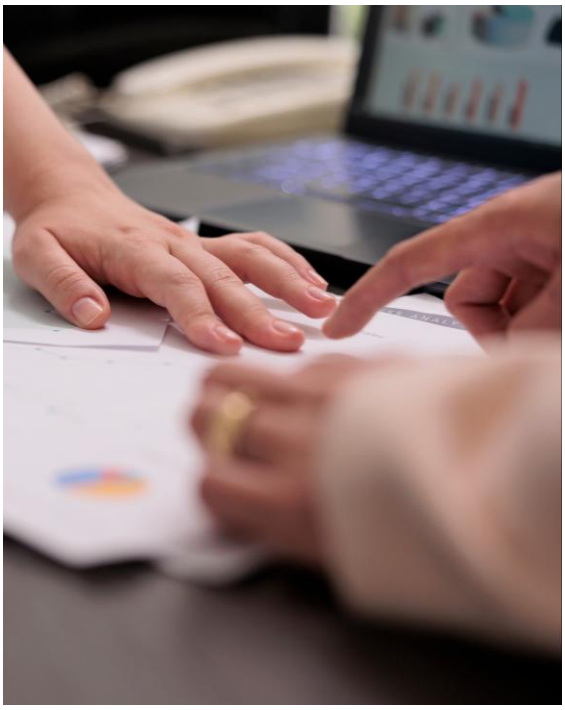
Beispiel: Es ist besser, ein Standardpasswort einer Appliance zu ändern, das einem Angreifer das Ausbreiten in Ihrem Netzwerk einfach macht, als eine komplexe Threat-Intelligence-Plattform einzukaufen, die Sie überhaupt nicht nutzen.

Weniger, dafür aber gezielte Maßnahmen, die echte Lücken schließen, sind immer wirksamer als planloser Aktionismus.

Kennzahlen, die wirklich zählen

Wenn Sie Klarheit wollen, müssen Sie das messen, was wirklich zählt.
Anstatt auszuwerten, wie viele Tools Sie haben oder wie viele Warnmeldungen Sie erhalten, erfassen Sie:

- Wie viele ausnutzbare Angriffspfade wurden beseitigt
- Wie schnell erkennen Sie einen Angriff erkennen und wie effektiv reagieren Sie darauf
- Wie gut widerstehen Ihre Nutzer Phishing-Angriffen
- Wie wiederherstellbar sind Ihre Daten nach einem Ransomware-Angriff



Das sind Klarheitsmetriken. Sie helfen Ihnen zu verstehen, ob Sie das richtige tun – nicht nur, ob Sie viel tun.

Fazit: Weniger tun. Aber dafür das Richtige.

Cybersicherheit für kleine Unternehmen muss nicht überwältigend sein. Die erfolgreichen Organisationen sind nicht diejenigen mit den meisten Tools, sondern jene mit dem klarsten Fokus, der konsequentesten Umsetzung und dem Mut zur Vereinfachung.

Wenn der Fokus stimmt, ist weniger zu tun keine Nachlässigkeit, sondern Disziplin. Es ist Führung. So erzielen kleine Teams große Wirkung.

Atmen Sie tief durch, treten Sie einen Schritt zurück und entscheiden Sie: Womit fangen Sie heute an (Start), was lassen Sie ab heute sein (Stop) und was vereinfachen Sie heute (Simplify)?

About us

Über die Autorin

Iva Lazić ist Cybersecurity-Beraterin mit Schwerpunkt auf Geschäftsentwicklung, Kundenmanagement und Ausbildung. Sie unterstützt Organisationen dabei, ihre Sicherheitspraktiken durch maßgeschneiderte Lösungen und Schulungen zu verbessern. LinkedIn

Über Cybovate

Cybovate liefert Cybersicherheitslösungen der nächsten Generation, die Komplexität in Klarheit verwandeln. Das Unternehmen ermöglicht Unternehmen ein proaktives Schwachstellenmanagement durch autonome Penetrationstests, risikobasierte Priorisierung und optimierte Berichterstattung. Mit dem Fokus auf messbare Ergebnisse und vereinfachte Entscheidungsfindung ermöglicht Cybovate seinen Kunden, Widerstandsfähigkeit aufzubauen, Risiken zu reduzieren und echtes Cybervertrauen zu erlangen. Erfahren Sie mehr unter cybovate.com.