K&P COMPUTER® BLUE CONSULT.

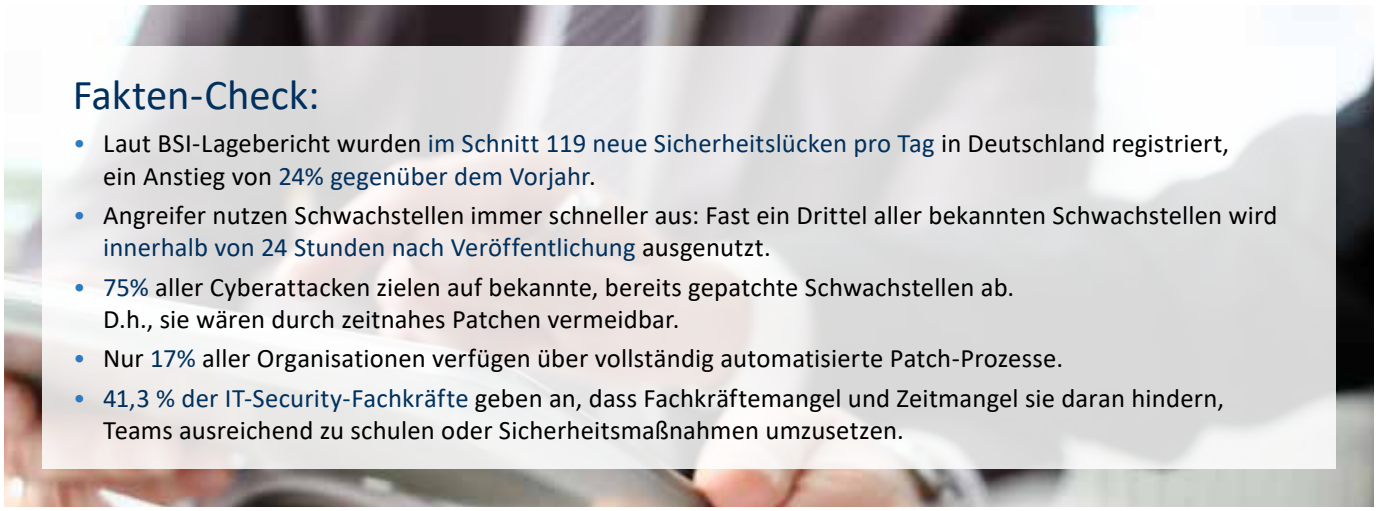
Managed Alert X

Nicht der Cyberangriff ist das Problem, sondern die fehlende Transparenz davor!

Wer Risiken nicht erkennt, kann sie nicht priorisieren oder beherrschen.

IT-Umgebungen werden komplexer, Herstellerinformationen immer unübersichtlicher und Bedrohungslagen dynamischer. Sicherheitslücken, fehlende Updates und schleichende Systemprobleme bleiben oft lange unentdeckt, bis es zu Ausfällen oder Sicherheitsvorfällen kommt.

Managed Alert X ist ein externer Expertenservice zur regelmäßigen Überprüfung und Bewertung Ihrer IT-Sicherheits-, Patch- und Systemrisiken, inklusive priorisierter Handlungsempfehlungen für IT-Leitung und Management.



Fakten-Check:

- Laut BSI-Lagebericht wurden im Schnitt 119 neue Sicherheitslücken pro Tag in Deutschland registriert, ein Anstieg von 24% gegenüber dem Vorjahr.
- Angreifer nutzen Schwachstellen immer schneller aus: Fast ein Drittel aller bekannten Schwachstellen wird innerhalb von 24 Stunden nach Veröffentlichung ausgenutzt.
- 75% aller Cyberattacken zielen auf bekannte, bereits gepatchte Schwachstellen ab. D.h., sie wären durch zeitnahes Patchen vermeidbar.
- Nur 17% aller Organisationen verfügen über vollständig automatisierte Patch-Prozesse.
- 41,3 % der IT-Security-Fachkräfte geben an, dass Fachkräftemangel und Zeitmangel sie daran hindern, Teams ausreichend zu schulen oder Sicherheitsmaßnahmen umzusetzen.

Quellen: Branchenumfragen, Statistiken

Wie ist die Lage bei Ihnen?

- Wissen Sie jederzeit, wie sicher und stabil Ihre Systeme aktuell betrieben werden?
- Haben Sie einen klaren, priorisierten Überblick über sicherheitsrelevante Warnungen, Updates und Risiken?
- Reagieren Sie proaktiv auf erkannte Risiken oder erst, wenn es bereits zu Störungen oder Ausfällen kommt?
- Müssen Hersteller-, Sicherheits- und Systemmeldungen manuell bewertet und zusammengeführt werden?
- Fehlen Ihrer IT oder Administration Zeit und Ressourcen, um regelmäßige Zustandsprüfungen durchzuführen?
- Haben Sie eine belastbare Entscheidungsgrundlage, um Wartungsmaßnahmen und Investitionen sinnvoll zu priorisieren?

Warum jetzt Handlungsbedarf besteht:

Sicherheitsrisiken entstehen nicht plötzlich, sie entwickeln sich schleichend und bleiben oft lange unentdeckt. Wer hier nicht kontinuierlich hinschaut, reagiert im Ernstfall unter massivem Zeitdruck, mit ungeplanten Maßnahmen und vermeidbaren Kosten.

Proaktive Überwachung schafft Handlungsspielräume, Planungssicherheit und Kostenkontrolle.

Unser Angebot:

Mit Managed Alert X übernehmen wir für Sie die regelmäßige technische Überprüfung Ihrer vertraglich definierten IT-Komponenten.

Enthaltene Leistungen:

- Monatlicher Health-Check
  - Prüfung auf technische Fehler, Auffälligkeiten und potenzielle Risiken
- Monatliche Prüfung der Patch- & Update-Stände
  - Abgleich mit Hersteller-Patches, Sicherheitsupdates und bekannten Schwachstellen
- Individueller Management-Report – **Managed Alert X**
  - **Übersichtlicher Monatsbericht per E-Mail**
    mit relevanten Sicherheitslücken, Warnmeldungen und kritischen Herstellerankündigungen
  - **Transparente Bewertung des aktuellen Systemzustands**
    inkl. Stabilität, Sicherheitsniveau und Auffälligkeiten
  - **Klar identifizierte Risiken und Handlungsbedarfe**
    verständlich eingeordnet und fachlich bewertet
  - **Konkrete, priorisierte Handlungsempfehlungen**
    als belastbare Entscheidungsgrundlage für IT und Management
- **Patch-Risiko:**
  Monatliche Prüfung der Patch- & Update-Stände
  - Abgleich mit Hersteller-Patches (Hersteller Security Advisories), Sicherheitsupdates und bekannten Schwachstellen (CVE-Datenbanken)

Wichtiger Hinweis:
Das Einspielen von Patches und Updates ist nicht automatisch Bestandteil von Managed Alert X.
Auf Wunsch übernehmen wir diese Leistungen separat, transparent und planbar nach Aufwand.

Für Wen ist das Angebot interessant?

Ideal für Unternehmen:

- Ohne eigenes Security-Team
- Mit kleiner IT
- Mit vielen Herstellersystemen
- Mit wenig Patch-Transparenz

Managed Alert X ist ein unterstützendes Werkzeug zur Verbesserung Ihrer IT-Sicherheit. Es ersetzt keine ganzheitliche Sicherheitsstrategie oder regelmäßige Prüfungen durch qualifizierte Fachleute. Wir empfehlen, weiterhin bewährte Sicherheitspraktiken anzuwenden und bei Bedarf auf die Expertise unserer Experten zurückzugreifen.

Benefits

- Frühzeitige Erkennung von Sicherheits- und Stabilitätsrisiken
- Reduzierung ungeplanter Ausfälle und Notfälle
- Klare, priorisierte Handlungsempfehlungen statt Informationsflut
- Planbare Maßnahmen statt Reaktion unter Zeitdruck
- Entlastung der internen IT durch ausgelagerte Analyse & Bewertung
- Bessere Entscheidungsgrundlagen für Wartung und Investitionen
- Planbare Kosten statt teurer Ad-hoc-Maßnahmen

Kontakt

Jens, Friedrich, Berta-Cramer-Ring 10, 65205 Wiesbaden
j.friedrich@kpc.de, Telefon: +49 6122 7071 0