DEFENDER BOX
EINFACH.SCHNELL.CYBERSICHER.

Kontaktieren Sie uns unter
defenderbox.de/kostenloser-test



DEFENDERBOX

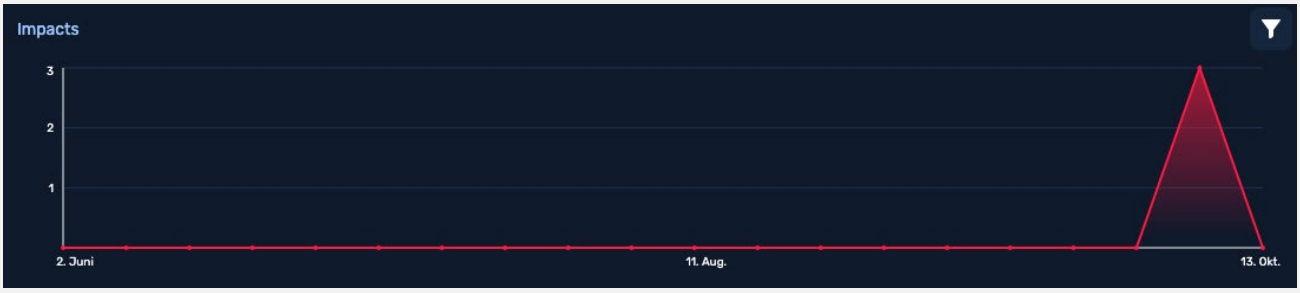
SUCCESS STORY

Managed Security Service für DRK Ahaus e.V.
Wöchentliche IT-Sicherheitsüberprüfungen,
weil es sich lohnt!

©SMB Cybersecurity GmbH

DEFENDERBOX
SUCCESS STORY

Deutsches Rotes Kreuz | Ortsverein Ahaus e.V.



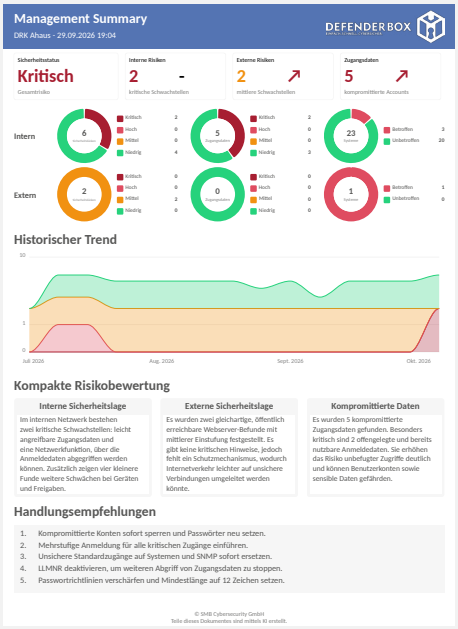
Montag: alles im grünen Bereich. Dienstag: zwei hochkritische Lücken.

Beim **DRK Ahaus e.V.** prüft die **DEFENDERBOX** jede Woche die IT-Infrastruktur. Monatelang waren die Ergebnisse durchweg zufriedenstellend.

Dann wurde ein neues Gerät eingebunden. Ein ganz normaler Vorgang, wie er überall vorkommt.

Bei der nächsten Prüfung meldete die **DEFENDERBOX** zwei hochkritische Sicherheitslücken. Ein einziges Gerät hatte die Angriffsfläche über Nacht verändert.

Weil wöchentlich geprüft wird, blieb das nicht lange unbemerkt. Die Lücken wurden erkannt, bevor sie jemand ausnutzen konnte. Bei einer jährlichen Prüfung wäre das womöglich erst Monate später aufgefallen.


Management Summary
DRK Ahaus - 29.09.2026 19:04
DEFENDERBOX
Sicherheitsstatus
Kritisch
Gesamtrisiko
Interne Risiken
2
kritische Schwachstellen
Externe Risiken
2
mittlere Schwachstellen
Zugangsdaten
5
kompromittierte Accounts
Intern
Extern
Historischer Trend
Kompakte Risikobewertung
Interne Sicherheitslage
Im internen Netzwerk bestehen zwei kritische Schwachstellen: leicht angreifbare Zugangsdaten und eine Netzwerkfunktion, über die Anmeldedaten abgegriffen werden können. Zusätzlich zeigen vier kleinere Funde weitere Schwächen bei Geräten und Freigaben.
Externe Sicherheitslage
Es wurden zwei gleichartige, öffentlich erreichbare Webserver-Befunde mit mittlerer Einstufung festgestellt. Es gibt keine kritischen Hinweise, jedoch fehlt ein Schutzmechanismus, wodurch Internetverkehr leichter auf unsichere Verbindungen umgeleitet werden könnte.
Kompromittierte Daten
Es wurden 5 kompromittierte Zugangsdaten gefunden. Besonders kritisch sind 2 offengelegte und bereits nutzbare Anmeldedaten. Sie erhöhen das Risiko unbefugter Zugriffe deutlich und können Benutzerkonten sowie sensible Daten gefährden.
Handlungsempfehlungen
1. Kompromittierte Konten sofort sperren und Passwörter neu setzen.
2. Mehrstufige Anmeldung für alle kritischen Zugänge einführen.
3. Unsichere Standardzugänge auf Systemen und SNMP sofort ersetzen.
4. LLMNR deaktivieren, um weiteren Abgriff von Zugangsdaten zu stoppen.
5. Passwortrichtlinien verschärfen und Mindestlänge auf 12 Zeichen setzen.

Fazit:
Eine IT-Infrastruktur ist nie ein fester Zustand. Jedes neue Gerät, jedes Update kann Risiken mitbringen. Gerade DRK-Einrichtungen, die sensible Daten verarbeiten und auf deren Dienste sich Menschen verlassen, brauchen kontinuierliche Überprüfungen als festen Bestandteil ihrer IT-Sicherheitsstrategie.

Sicherheit ist kein Haken auf einer Checkliste, sondern ein laufender Prozess.
defenderbox.de/kostenloser-test