# Schwachstellen-Hypes: Security-Teams und die richtige Kommunikation

Einige Schwachstellen des vergangenen Jahres schafften es bis in die Schlagzeilen der Tagespresse: Rund um Meltdown, Spectre oder Struts 2 entstand ein regelrechter medialer Hype. Damit wurden selbst Unternehmensbereiche darauf aufmerksam, die sonst nichts mit Schwachstellen-Management zu tun haben: Geschäftsführung, Investor Relations, Kundenservice oder Unternehmenskommunikation.

Tenable erklärt, wie Sicherheitsteams auf Fragen dazu reagieren können.

- Mediale Aufmerksamkeit ist kein Maßstab, um die tatsächlichen Gefahren einzuschätzen, denn Medien berichten über interessante Schwachstellen – nicht nur die tatsächlich kritischen. Security-Teams bewerten Risiken aber nicht nach medialer Aufmerksamkeit. Sie sollten die verschiedenen Verantwortlichen stattdessen darüber aufklären, wie sie selbst diese Risiken beurteilen und worauf diese Einschätzung basiert. Außerdem müssen sie akzeptieren, dass auch weniger dringliche Schwachstellen unter Umständen eine Reaktion erfordern. Sollten sie die Erwartungen nach einer schnellen Lösung oder Reaktion noch nicht erfüllen können, müssen sie dies ebenfalls erläutern.

- Security-Teams sollen die erkannten Risiken einordnen und alle Betroffenen dazu beraten. Das gilt besonders für Entscheidungsträger: Denn von deren Warte aus betrachtet sind Schwachstellen oft „politisch“ – sie können dem Ansehen des Unternehmens schaden, selbst wenn die tatsächlichen, technischen Gefahren viel geringer sind, als die dadurch entstehende Aufregung vermuten lässt. Teams müssen in diesen Fällen kontextbasierte Antworten parat haben – und sich nicht vom Hype verrückt machen lassen. Entscheidend ist, dass die Security-Experten die Erkenntnisse aktuell kommunizieren und die teils komplexen, theoretischen Sachverhalte den Laien erklären.

**Fazit**
Beim Umgang mit Schwachstellen ist die Art der Kommunikation entscheidend: Nachrichten und umfassende Berichterstattung können für Unruhe sorgen – selbst, wenn eine Schwachstelle noch gar nicht ausgenutzt wurde oder keine weiteren Details dazu vorliegen. Landet eine Schwachstelle einmal in den Schlagzeilen, ist es an der Zeit, aktiv verschiedene Geschäftsbereiche ins Boot zu holen. So zeigen Security-Teams, dass sie alles im Griff haben und bauen Vertrauen auf, das bei der nächsten Hype-Schwachstelle die größte Unruhe verhindert.