

PRESSEMITTEILUNG

Nur ein Drittel deutscher Unternehmen ausreichend auf DDoS-Attacken vorbereitet

Umfrage von Link11 und TeleTrust - Bundesverband IT-Sicherheit e.V.

Berlin, 31.10.2016 - Im Rahmen der it-sa 2016 führte Link11 in Kooperation mit TeleTrust eine Umfrage unter 250 IT-Entscheidern und -Beratern durch. Aktueller Hintergrund war die umfassende DDoS-Attacke auf den DNS-Service des Anbieters dyn, die u.a. zu Serviceausfällen bei Twitter, New York Times und Netflix führte. Während nur 60 % der Unternehmen selbst von einer steigenden Gefahr durch DDoS ausgehen, sind sich 76,5 % der Berater sicher, dass das Risiko in den kommenden 12 Monaten Opfer einer DDoS-Attacke zu werden, weiter zunehmen wird.

Über 34 % der befragten Unternehmen gaben an, bereits einmal Opfer einer DDoS-Attacke gewesen zu sein. Bei den Beratern waren es über 61 % ihrer Kunden. Beide Gruppen geben an, dass die Angreifer es nicht bei einem Angriff belassen. 35,4 % der befragten Unternehmen waren schon mehr als 10 Angriffen ausgesetzt. Fast ¼ der befragten Unternehmen sehen die Zuständigkeit für den DDoS-Schutz beim eigenen Unternehmen. Trotzdem verlassen sich nur 39 % der Unternehmen auf dedizierte Schutzlösungen mittels Hardware oder Cloud-Schutz. Die befragten IT-Berater gaben an, dass nur 35,29 % ihrer Kunden planen, innerhalb der nächsten 12 Monate einen DDoS-Schutz zu implementieren. 21 % der befragten Unternehmen gaben an, bereits Erpressermails erhalten zu haben, 27,8 % Unternehmen waren noch nicht betroffen, kannten jedoch bereits ein betroffenes Unternehmen. Bei den Beratern waren bereits 32,1 % der Kunden betroffen. Bei der Frage, ob das Unternehmen im Falle einer Erpressung "Schutzgeld" zahlen würde, ergab sich eine überraschende Diskrepanz zwischen Unternehmen und Beratern. Während 86,7 % der Unternehmen niemals zahlen würden, glaubten gerade einmal 38 % der Berater, dass ihre Kunden nicht zahlen würden. 47,5 % gehen davon aus, dass ihre Kunden auch im Notfall z.B. eine Bitcoin-Zahlung an Erpresser senden würden.

TeleTrust - Bundesverband IT-Sicherheit e.V.

Der Bundesverband IT-Sicherheit e.V. (TeleTrust) ist ein Kompetenznetzwerk, das in- und ausländische Mitglieder aus Industrie, Verwaltung, Beratung und Wissenschaft sowie thematisch verwandte Partnerorganisationen umfasst. Durch die breit gefächerte Mitgliedschaft und die Partnerorganisationen verkörpert TeleTrust den größten Kompetenzverbund für IT-Sicherheit in Deutschland und Europa. TeleTrust bietet Foren für Experten, organisiert Veranstaltungen bzw. Veranstaltungsbeteiligungen und äußert sich zu aktuellen Fragen der IT-Sicherheit. TeleTrust ist Träger der "TeleTrust European Bridge CA" (EBCA; PKI-Vertrauensverbund), der Expertenzertifikate "TeleTrust Information Security Professional" (T.I.S.P.), "TeleTrust Engineer for System Security" (T.E.S.S.) und "Certified Professional for Secure Software Engineering" (CPSSE) sowie des Qualitätszeichens "IT Security made in Germany". TeleTrust ist Mitglied des European Telecommunications Standards Institute (ETSI). Hauptsitz des Verbandes ist Berlin.