Die (erste) Ruhe nach dem Sturm nutzen:
Sophos-Checkup für die Cloud-Sicherheit in Unternehmen

Die Pandemie hat schon ordentlich etwas angezettelt auf der Welt. Was den IT-Bereich angeht, dürfte ein geflügeltes Wort aus dem Silicon Valley wohl am ehesten beschreiben, was IT-Teams rund um den Globus zu leisten hatten: "Das Flugzeug bauen, während es fliegt." Ohne Zeitverzögerung galt es in der Lockdown-Situation plötzlich, unzählige neue Remote-Arbeitsplätze zu ermöglichen, um Geschäftskontinuitäten zu gewährleisten. Ein Schlüssel-Instrument bei alledem: Die Cloud. Die Nutzung von Cloud-Diensten ist seit März sprunghaft angestiegen und verbindet Infrastruktur, Menschen, Geräte, Anwendungen und Informationen auf eine Art und Weise, die wir uns vorher kaum hätten vorstellen können. Tatsächlich hätten auch die IT-Teams in Unternehmen, Behörden und Organisationen, die für die Aufrechterhaltung des Geschäftsbetriebs gesorgt haben, den einen oder anderen Applaus verdient.

Ging es im März dabei vor allem darum, in Unternehmen die IT-Infrastruktur sicherzustellen, die notwendig ist, um auch in Lockdown-Zeiten den Betrieb aufrecht zu erhalten, gilt es heute, den sicheren Weiterbetrieb zu gewährleisten. Jetzt, da wieder ein beinahe normaler Arbeitsalltag einsetzt – Menschen kehren in ihre Büros zurück, zahlreiche andere haben sich gut im Homeoffice eingerichtet – ist ein guter Zeitpunkt, die Cloud-Setups zu überprüfen und gegebenenfalls das, was seinerzeit aus zeitlichen Gründen nicht perfekt umgesetzt werden konnte, zu korrigieren.

Fehler korrigieren, Sicherheitslücken schließen
Bereits vor der Pandemie erwiesen sich laut SophosLabs Threat Report mit 66 Prozent die Fehlkonfigurationen als Hauptursache für Angriffe – und diese sind weltweit zahlreich: Die jüngste Sophos Umfrage zum Thema Cloud, The State Of Cloud Security, zeigte, dass fast drei Viertel (70 Prozent) der Unternehmen weltweit im letzten Jahr einen Cloud-Sicherheitsvorfall zu verzeichnen hatten. Hierzu gehörten Angriffe von Lösegeld- und anderer Malware, ungeschützte Daten und kompromittierte Konten. In Deutschland waren rund sechs von zehn Unternehmen, die Public-Cloud-Dienste nutzen, von Vorfällen betroffen. Und meist kamen die Angreifer in die öffentliche Cloud-Umgebung, weil Unternehmen eben versehentlich quasi ein Fenster offen oder die Schlüssel in der Tür stecken ließen.

Die Sicherheit in der Cloud in die Hand nehmen
Security ist ein kontinuierlicher Prozess, bei dem es darum geht, Cloud-Umgebungen ständig zu verwalten und zu überwachen, um möglichen Angreifern immer einen Schritt voraus zu sein. Die Verantwortung für die Sicherheit der Cloud teilen sich Unternehmen und Cloud-Service-Provider. Im Wesentlichen ist der Cloud-Anbieter dabei für den physischen Schutz im Rechenzentrum und die virtuelle Trennung von Kundendaten und Umgebungen verantwortlich. Die Sicherheit der Unternehmensdaten, die in der Cloud ausgeführt oder gespeichert werden, liegt jedoch in der Hand der Unternehmen selbst. Es gilt, diese Mitverantwortung wahrzunehmen. Es gibt einige grundlegende Sicherheitsmaßnahmen, die Unternehmen nun vornehmen können und sollten, um ihre Vermögenswerte in der Cloud zu schützen.

Checkliste zur Prüfung der Cloud-Sicherheit:

- Überblick verschaffen: was wird genutzt, wo befindet es sich, wer hat Zugriff darauf, gibt es Sicherheitslücken?

- Die Gefahrenlage kennen. Unternehmensdaten in der Cloud sind für Hacker grundsätzlich von Interesse. Sie führen Scans durch, und wenn sie Lücken finden oder die Zugangsdaten eines Mitarbeiters zur Cloud in die Hände bekommen haben, werden sie das nutzen.
- Genaue Überprüfung der Konfigurationen. Etwaige Fehlkonfigurationen korrigieren und damit mögliche Einstiegsluken für Angreifer schließen.
- Kritische Prüfung von Zugriffsberechtigungen. Zugang sollten nur die Mitarbeiter haben, die ihn auch tatsächlich benötigen.
- Festlegung von Authentifizierungsanforderungen. Multi-Faktor-Authentifizierung in den Cloud-Provider-Accounts nutzen. Je schwieriger der Zutritt, desto sicherer ist er.
- Gleichbehandlung aller Komponenten: Virtuelle Remote-Desktops unter den gleichen Sicherheitsaspekten behandeln wie die wichtigsten Unternehmens-Server.
- Sichere Verbindungen für den Zugriff auf Anwendungen und Unternehmensdaten schaffen. Unabhängig davon, ob die betreffenden Mitarbeiter an ihren Arbeitsplatz zurückgekehrt sind oder vorerst an einem entfernten Standort bleiben werden.
- Mehrschichtige Sicherheitssoftware einsetzen zum Schutz von Cloud-Workloads.

Pressekontakt:

Sophos
Jörg Schindler, PR-Manager Central & Eastern Europe
joerg.schindler@sophos.com, +49-721-25516-263

TC Communications
Arno Lücht, +49-8081-954619
Thilo Christ, +49-8081-954617
Ulrike Masztalerz, +49-30-55248198
Ariane Wendt +49-172-4536839
sophos@tc-communications.de