PRESSEMITTEILUNG

Interview

BSI-Lagebericht 2017: Experte rät zur Prüfung des Active Directory

- Sicherheitslage für IT-Systeme laut BSI angespannt
- Angreifer haben es auf Benutzerverwaltung abgesehen
- Interview mit Frank Greding, Comma Soft AG

Bonn, 15.11.2017 – Die Situation bleibt angespannt: In seinem neuen Bericht zur Informationssicherheit warnt das Bundesamt für Sicherheit in der Informationstechnik (BSI) vor der prekären Sicherheitslage von IT-Systemen in Deutschland. Demnach haben Cyber-Kriminelle insbesondere mit sogenannter Ransomware ein lukratives Geschäftsmodell entdeckt und entwickeln stetig neue Erpressungssoftware. Dadurch wächst das Spektrum unterschiedlicher Angriffsmethoden rasant. Laut Frank Greding, Competence Center Manager Backend & Security Services beim Software- und IT-Consulting-Spezialisten Comma Soft, gilt es für Unternehmen, das Active Directory (AD) regelmäßig auf Schwachstellen zu prüfen. Denn: Der Windows-basierte Verzeichnisdienst steht oft im Fadenkreuz krimineller Angriffe.

Frage: Laut des neuen Lageberichts des BSI ist die Zahl der Cyber-Attacken unverändert hoch. Warum haben es viele der Angreifer auf das Active Directory eines Unternehmens abgesehen?

Greding: Das AD eines Unternehmens ist der zentrale Dreh- und Angelpunkt für zahlreiche weitreichende Prozesse. Es steuert sogar oftmals nicht nur die Zugänge zu Dateidiensten, sondern auch zu business-kritischen Applikationen, ERP- und Cloud-Services sowie Webdiensten. Die Angreifer versuchen, Zugriffsrechte zu erlangen und zu ihren Gunsten auszuweiten. Das AD ist damit das Einfallstor, um im Unternehmen massiven Schaden anzurichten. Es verwundert also nicht, dass das Active Directory das Ziel eines jeden Angriffs ist, der nicht unmittelbar den Ausfall eines Services herbeiführen soll.

Frage: Wie können Unternehmen ihr AD am besten vor Attacken schützen?

Greding: Ähnlich wie mit einem Penetration Test durch ethische Hacker in Bezug auf die präventive IT-Sicherheit macht es Sinn, auch das AD eines Unternehmens auf Schwachstellen zu untersuchen. Dazu empfiehlt sich eine umfassende Überprüfung der Benutzerverwaltung.

Frage: Wie läuft eine solche Prüfung ab?

Greding: Experten untersuchen dabei in der Regel die Dimensionen „Mensch“, „Prozesse“ und „Technologie“, um einen ganzheitlichen Blick auf die Problematik zu erhalten. Denn was nützt es, wenn Technologie und Prozesse auf dem neuesten Stand und optimal konfiguriert sind, aber die Mitarbeiter nicht über entsprechendes Knowhow verfügen? Die Kenntnisse der verantwortlichen Belegschaft können in Interviews abgefragt werden.

Frage: Wie viel Zeit nimmt eine solche Überprüfung in Anspruch und welcher Aufwand kommt auf das Unternehmen zu?

Greding: Die erforderliche Zeit differiert von Fall zu Fall und ist abhängig von den vereinbarten Prüfungen. Die Prüfung kann beispielsweise auf Sicherheitsthematiken fokussiert sein oder den AD-Service betreffen. Während der Untersuchung werden deswegen unter anderem Interviews mit verschiedenen Mitarbeitern, z.B. Domänenadministratoren, dem AD-Service-Desk etc., geführt.

Frage: Was passiert, wenn Sicherheitsrisiken entdeckt werden?

Greding: Nach dem Fever Check, wie die Comma Soft AG eine solche Prüfung nennt, erhält das Unternehmen einen genauen Bericht über die Ergebnisse. Diese orientieren sich an dem internationalen Standard CMMI (Capability Maturity Model Integration). Es sind aber auch individuelle Bewertungsmodelle je nach Unternehmen denkbar. Für ein Untersuchungsergebnis auf ganzheitlicher Basis werden jedoch immer alle relevanten technischen und prozessbezogenen Aspekte genauso wie die menschlichen Faktoren mit einbezogen. Auf dieser Grundlage können gezielt Empfehlungen zur Optimierung eines AD ausgesprochen werden.

Frage: In welcher Häufigkeit empfehlen Sie diese Maßnahmen?

Greding: Auch nach einer ersten Prüfung des AD sollte man die Risiken nicht unterschätzen. Es ist ratsam, ein AD alle 18 bis 24 Monate erneut einem Fever Check zu unterziehen, da es viele Faktoren gibt, die sich in dieser Zeit ändern können. In manchen Fällen lohnt es sich auch, ein neues AD aufzusetzen und Experten bereits während der Planung in Anspruch zu nehmen. Dadurch kann eine State-of-the-Art-Implementierung gewährleistet werden, um alle Sicherheitsmechanismen des neuen Releases von Anfang an zu nutzen.

Frage: Unter welchen Voraussetzungen empfiehlt sich eine vollständig neue Implementierung eines AD?

Greding: Besonders bei großen Traditionsunternehmen, bei denen über Jahrzehnte des Wachstums neue Mitarbeiter, Abteilungen oder Standorte in die IT-Landschaft integriert werden mussten, kommt es häufig zu komplexen und teils redundanten AD-Strukturen. In solchen Fällen ist es meist am effektivsten, das Verzeichnis gänzlich neu aufzusetzen.

Über Frank Greding:

Frank Greding ist Competence Center Manager Backend & Security Services bei der Comma Soft AG, einem Bonner IT-Unternehmen mit Fokus auf Data Business-, IT-Consulting und Softwareentwicklung. Gredings Schwerpunkt liegt auf der Beratung zur Informationssicherheit der Active Directory von Unternehmen.

Weitere Infos:
https://www.comma-soft.com/

Über die Comma Soft AG:

Die Comma Soft AG – „The Knowledge People“ wurde 1989 von Stephan Huthmacher gegründet. Seitdem hat sich das Unternehmen einen Namen als „Digital Think Tank“ und innovatives IT-Consulting- und Software-Haus gemacht. Comma Soft unterstützt Kunden bei der Umsetzung der digitalen Transformation ihrer Geschäftsmodelle. Das Leistungsspektrum umfasst Data Science-, Analytics-, IT-Strategie, IT-Architektur und Security-Consulting sowie die dazu passenden Software-Produkte und Lösungen. Sowohl große und mittelständische Unternehmen in der DACH-Region als auch zahlreiche DAX-Konzerne bauen auf die 27-jährige Erfahrung von Comma Soft im Enterprise-Umfeld. 135 Mitarbeiter sorgen am Stammsitz in Bonn und bei den Kunden vor Ort dafür, dass Projekte agil und wertschöpfend umgesetzt werden.

Kontakt für Journalisten & Redaktionen:

Malte Limbrock
Sputnik GmbH
Presse- und Öffentlichkeitsarbeit
Lessingstraße 60
53113 Bonn
Tel.: +49 (0)228 / 30412-630
Fax: +49 (0)228 / 30412-639
limbrock@agentur-sputnik.de
www.sputnik-agentur.de

Hagen Thiele
Sputnik GmbH
Presse- und Öffentlichkeitsarbeit
Lessingstraße 60
53113 Bonn
Tel.: +49 (0)228 / 30412-633
Fax: +49 (0)228 / 30412-639
thiele@sputnik-agentur.de
www.sputnik-agentur.de