Wie Log- und Power-Management vor Angriffen schützen

Mithilfe von Log- und Power-Management ist es möglich, ein BCM-System aufzubauen, das auch im Krisenfall für Sicherheit sorgt, ohne das Budget zu sprengen.

Von Jürgen Kolb, iQSol

Um Gefahren und mögliche Angreifer frühzeitig zu erkennen, benötigen Unternehmen ein effizientes Log-Management. Ob übermäßig viele Log-in-Versuche auf dem Server oder massenweise anonyme Zugriffe auf die eigene Website: Diese Anzeichen werden mithilfe von Logs und deren Korrelationsmechanismen sichtbar – was ein schnelles Eingreifen erlaubt.

Integrieren Betreiber kritischer Infrastrukturen zusätzlich noch ein Alarmierungssystem, kann das die Verteidigung gegen Cyberangreifer abermals beschleunigen. Wie im Vorbeigehen werden dabei auch noch weitere Themen erledigt: Seien es Standards wie ISO 22301 oder PCI-DSS – selbst der neuen Datenschutzgrundverordnung wird man in Bezug auf eine sichere Protokollierung, rechtliche Meldepflichten und vollständige Reports gerecht. Das gilt auch für mittlerweile immer häufiger in die IT-Welt gebrachte Energiesysteme wie Smartmeter oder die seit Jahrzehnten bestehenden Systemanlagen, die nun erneuert werden. Sie werden genauso gesichert wie Windows- oder Linux-Server in Rechenzentren. Eine große Herausforderung ist jedoch das Absichern von Systemen, die in der IT-Welt längst tot sind, wie zum Beispiel Windows XP.

Kurzschlusshandlungen haben keinen Sinn

Aller Innovation und gesetzlichen Bestimmungen zum Trotz macht es wenig Sinn, schnell und unüberlegt zur nächstbesten Absicherung zu greifen. Doch wenn der Handlungsschmerz sehr groß ist und die Bereitschaft der Konzernleitung für notwendige Investitionen steigt, ist die Anschaffung einer teuren Software-Lösung, die hoch spezialisiert auf Trojaner und Bot-Netze losgeht, die Praxis. Oft handelt es sich dabei sogar um ein Security-Information-and-Event-Management-(SIEM)-System oder um eine Malware-Protection-Software. Die Lösungen helfen jedoch wenig, wenn das Personal fehlt oder es nicht über das nötige Know-how verfügt. Auch wenn solche Systeme ungenügend in die organisatorisch-technischen Kerngeschäfte eingebunden sind, ist der Nutzen eher gering. Bei einem modifizierten Angriff sind dann diejenigen Unternehmen, auf die die vorangegangene Schilderung zutrifft, mit großer Wahrscheinlichkeit wieder betroffen, denn die vielfältigen Ursachen wie die „Awareness" der Mitarbeiter oder technische Probleme, wie eine schwache E-Mail-Security oder fehlende Sandbox-Techniken, wurden bei der Einführung des Systems nicht analysiert.

Abbildung 1: Ob Energiesysteme, Produktionsanlagen oder lebenswichtige Verteilsysteme: Die IT-Security nimmt die Herausforderung an und integriert sie. Bild: theyok/Fotolia.com

Da es nur wenig sinnvoll ist, für jeden IT-Security-Bedarf eine separate Software-Lösung anzuschaffen, kann nur eine zentralisierte und gut betreute Lösung der richtige Ansatz sein. Basis-Features werden darin dann optimiert und individuell eingestellt, im Zweifelsfall nachgeschärft und die Richtlinien durchgesetzt. So ist auch ein gesamtheitliches Monitoring möglich, das vor allem dann den Mehrwert gegenüber isolierten Applikationen bietet, wenn geräte- und herstellerübergreifend

Logiken greifen, alarmieren oder selbstständig handeln. Wenn jedoch darüber hinaus strategische Entscheidungen ausbleiben, die zum Beispiel ein automatisiertes Patchen und Scannen genauso vorsehen wie regelmäßige Pentests, wird auch eine zentrale Lösung die Sicherheit nicht erhöhen.

Kommunikation ergänzt Technik

Vor allem Business-Continuity-Manager benötigen daher neue Werkzeuge, die weit über die bisherigen Entscheidungsbefugnisse und Verantwortungsbereiche hinausgehen. Das verlangt eine abteilungsübergreifende Abstimmung, aber auch eine neue operative Aufwertung. Denn wer entscheidet im Notbetrieb, ob wichtige Teilsysteme bereits hochfahren, während der Blackout noch andauert? Was passiert, wenn die Dauer der USV-Systeme doch kürzer ist als geplant? Bedenkt man zudem die möglichen Ursachen für Stromausfälle, die von Kabelbrüchen über Brandalarme, Hacker-Attacken bis hin zu Unwetterkatastrophen oder Sabotage reichen, wird deutlich, dass schnelle Entscheidungswege gefragt sind, die sich auch im Zeitablauf widersprechen können. Im Vordergrund stehen meist die physische Unversehrtheit der Hardware und das Verhindern des unvermittelten Absturzes zur Verhinderung eines Datenverlustes.

Dafür muss auch die Frage geklärt sein, wer im Krisenfall zuständig ist, denn ohne Strom und ohne E-Mail-Konto kann er nicht erst informiert werden, sondern muss wissen, dass nun sein Einsatz gefragt ist. Ein Alerting-Notification-System, wie es bereits angesprochen wurde, stellt auch diese Kommunikation sicher, ganz gleich, welche Form des Notfalls eintritt. Ein offenes System kann hier Alarme verteilen, entgegennehmen, die Lokalität der Personen bestimmen und alle Vorgänge dokumentieren. Natürlich sollte ein Alarmierungssystem nicht nur im seltenen Fall des Alarmierens bereitstehen, sondern sich auch für Anforderungen eignen, wo die Fähigkeit gefragt ist, sich über SMS (Passwörter, Geo-Informationen) oder Apps zu informieren.

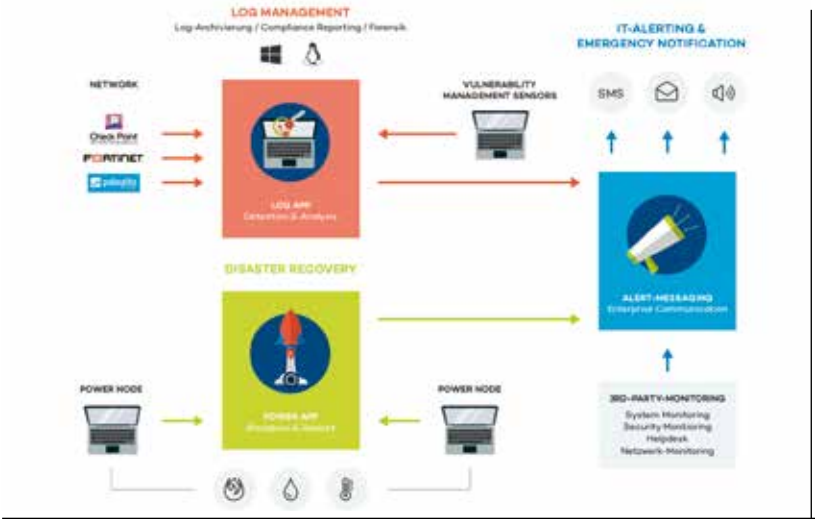

Abbildung 2: Was es braucht, sind gesamtheitliche Prozesse in der IT, die nicht bei der Security, sondern beim erfolgreichen Wiederanlauf des Rechenzentrums enden, wenn die Gefahr gebannt ist. Bild: Antares-NetlogiX

Was, wenn doch?

Trotz aller Vorkehrungen kann es dennoch passieren, dass ein Angreifer schneller ist als die Technologie und einen Schleichweg in die gut geschützten Systeme eines KRITIS-Unternehmens findet. Dann hilft nur eines: ein Power-Management. Eine an Systeme, Server und andere Maschinen angeschlossene Software-Logik mit empfohlener Appliance und Sensoren erlaubt es, diese nach einem vorab definierten Plan geordnet und in Abhängigkeit voneinander auf Knopfdruck herunter- und nach Vorübergehen der Gefahr wieder hochzufahren. Insbesondere bei Angriffen, die auf die Stromversorgung abzielen, ist das hilfreich, verursachen USVs oder Dieselaggregate mit ihrer Endlichkeit und vor allem Anfälligkeit so doch keine Bauchschmerzen mehr. Nichts stürzt mehr „einfach so“ ab, weil der Saft ausgeht. Aufgrund der Herausforderungen bei der Stromverteilung und Energiespeicherung ist gerade hier der Energiesektor sensibilisiert.

Aufgehoben ist damit allerdings nicht die Problematik des fehlenden ausgebildeten Personals. Unter anderem deswegen, aber auch aus Kostengründen, entscheiden sich zunehmend mehr KRITIS-Unternehmen für den Bezug von IT-Sicherheit als Dienstleistung. Managed-Security-Services stellen sicher, dass ein gesamtheitliches Sicherheitswissen rund um Software, aber vor allem auch zu angrenzenden Themen wie Datenschutz, Notfallhandbücher, Penetrationstests und mehr außerhalb des Unternehmens für den Schutz innerhalb des Unternehmens sorgt.

Rundumsicht

Mit zwei Systemen hat man nun ein umfangreiches Business-Continuity-Management geschaffen, das eine 360°-Sicht auf die wichtigen IT-Vorkommnisse eines KRITIS-Unternehmens zulässt. Denn mit einem ergänzenden Log-Management ist auch die zentrale Plattform für ein Informationssicherheits-Managementsystem (ISMS) geschaffen, das den Prozess „Abwehr, Alarmierung, Shutdown, Wiederanlauf“ abbilden kann. Wird hier ausschließlich auf Formular-Software gesetzt, wird bewusst die menschliche Komponente und somit eine zusätzliche Gefahrenquelle in Kauf genommen. Denn die technisch-organisatorischen Maßnahmen wie IT-Shutdown, Desaster-Simulationen und Auditierung sind nur dann wirklich sicher, wenn sie von einer Software gesteuert werden.