SOPHOS
Cybersecurity made simple.

Sophos sorgt für IT-Sicherheit bei 21 Bundesliga-Vereinen

Von den Profis für die Profis

IT-Sicherheit und Fußball. Zwei Themen, die auf den ersten Blick scheinbar so gar nichts miteinander zu tun haben, bei näherem Hinschauen aber überraschende Parallelen aufweisen. Dass zwischen den IT-Security-Lösungen von Sophos, die bei insgesamt 21 Profivereinen in Deutschland mit über 5.000 Lizenzen zum Einsatz kommen, und der Fußballstrategie so manche Verbindung besteht, macht eine kurze Analyse der gängigsten Fußballweisheiten schnell deutlich.

Wir müssen kompakt stehen!

Die Räume im Verbund dicht machen, um gegnerische Angriffe zu unterbinden. Genau das macht Sophos Synchronized Security. Allen voran das Feature Security Heartbeat, das durch eine innovative Verbindung zwischen Endpoints und Firewall den Austausch wichtiger Detailinformationen ermöglicht und IT-Sicherheit auf diese Weise komplett neu definiert. IP-Adressen sorgen für eine einfache Kommunikation zwischen Computern, aber sie machen es IT-Mitarbeitern alles andere als einfach, kompromittierte Computer ausfindig zu machen. Dank Security Heartbeat liegen Ihrer Firewall alle Informationen vor, die Sie benötigen, um schnell zu reagieren: der Name des sich verdächtig verhaltenden Computers, der angemeldete Benutzer und der Dateipfad des Prozesses, der schädlichen Datenverkehr sendet. So können Sie Ihre Zeit nutzen, um das Problem zu beheben, und nicht um nachzuforschen, woher das Problem stammt.

Wir setzten auf kontrollierte Offensive!

Wer das Spiel gestalten will, darf sich nicht nur auf seine rein defensiven Tugenden verlassen. Das proaktive Untersuchen scheinbar harmloser IT-Prozesse ist ein wichtiger Baustein zum Erfolg. Viele Vereine nutzen deshalb die brandneue Sophos-Technologie Intercept X. Sophos Intercept X verhindert unbefugte Spontanverschlüsselungen durch Ransomware mit CryptoGuard – selbst wenn es sich um vertrauenswürdige Dateien oder manipulierte Prozesse handelt. Nachdem Ransomware abgefangen wurde, versetzt CryptoGuard Ihre Dateien wieder in ihren sicheren Ursprungszustand zurück. Getreu dem Motto „Nach dem Spiel ist vor dem Spiel“ gibt zudem eine eingehende, forensikbasierte Analyse Aufschluss über die Ursache von Angriffen sowie deren Infektionswege und bietet detaillierte Anweisungen zur Beseitigung von Infektionen und zur Vorbeugung zukünftiger Risiken.

Die müssen mehr über Außen spielen!

Das Einbinden der Außenstellen ins Spiel ist ein elementarer Bestandteil für viele Unternehmen – auch in der Bundesliga. Dort lösen Sophos-Kunden das Problem mühelos mit Sophos Wireless Protection. Mit der Technologie können Unternehmen ihre WLAN-Infrastruktur einfach und sicher zur Verfügung stellen, indem sie ihre Sophos Firewall oder UTM als Wireless Controller zur zentralen Verwaltung und Sicherung des WLANs nutzen. Die Access Points werden von der Firewall automatisch eingerichtet und konfiguriert – ein Briefing durch den Trainer ist nicht mehr notwendig. So sind auch alle Wireless Clients zuverlässig vor Bedrohungen geschützt. Dabei sind die Sophos APs ohne Aufwärmzeit innerhalb weniger Minuten einsatzbereit und benötigen keine lokale Konfiguration.

Wir haben nicht nah genug am Mann gestanden!

Effektive Manndeckung entspricht in der IT-Security-Welt der Sicherung aller Endpoints – ohne den Überblick zu verlieren! Auch im Fußball setzen immer mehr Kunden von Sophos auf das Endpoint-Protection-Paket. Die Lösung blockiert Malware und Infektionen, indem sie bestimmte Techniken und Verhaltensweisen, die bei praktisch allen Exploits zum Einsatz kommen, erkennt und abwehrt. Da Sophos Endpoint Protection sich bei der Abwehr von Malware nicht auf Signaturen verlässt, werden Zero-Day-Bedrohungen abgefangen, ohne die Geräte-Performance zu beeinträchtigen. So verhindert Sophos Endpoint Protection bereits im Vorfeld, dass Exploits ausgenutzt werden können. Durch die Korrelation von Hinweisen auf Bedrohungen kann Sophos Endpoint Protection Web- und Anwendungs-Exploits, gefährliche URLs, potenziell unerwünschte Anwendungen und Schadcode proaktiv von Ihren Endpoints fernhalten.

Standardsituationen sind immer gefährlich!

Alle wissen, jetzt wirds gefährlich – und trotzdem passiert es immer wieder. Was bei Freistößen gang und gäbe ist, gilt auch für Phishing-Attacken, also das Verleiten zum Klicken auf einen bestimmten Link, der dann auf eine kriminelle oder mit Schadsoftware versehene Seite führt. Mehrere Bundesliga-Vereine schützen sich mit Sophos Enduser Protection and Mail vor diesen Attacken. Mit den Standardeinstellungen erhalten Unternehmen sofortigen Schutz für ihre Posteingänge, denn alle E-Mails mit verdächtigen Inhalten, Anhängen oder URLs werden automatisch abgefangen. Sophos Email Protection nutzt modernste Technologien zur Erkennung von Malware und Phishing, die kontinuierlich aktualisiert werden, um selbst neueste Bedrohungen rechtzeitig zu stoppen. Wenn ein E-Mail-Server ausfällt oder ein cloudbasierter Service von einer Störung betroffen ist, verschiebt Sophos Email Protection alle eingehenden E-Mails automatisch in eine Warteschlange, bis der Server wieder online geht. Sobald der Service wieder online geht, werden alle E-Mails aus der Warteschlange sicher zugestellt.

Im Pokal gibt es keine leichten Gegner!

Der „Pokal-Fight" ist für die IT-Sicherheit der tägliche Kampf gegen millionenfach auftretende Malware-Attacken, bei denen auch der kleinste Virus als Einfallstor sehr gefährlich werden kann. Entsprechend ist eine Rundum-Absicherung über alle Einfallstore notwendig. Zu diesem Zweck bauen viele Profivereine auf Sophos Access Points, um ein leistungsfähiges und sicheres WLAN-Netz zu garantieren. Die Sophos APs können innerhalb weniger Minuten eingerichtet werden und benötigen keine lokale Konfiguration. Der Controller wird automatisch gefunden, dessen IP-Adresse über DHCP abgerufen und die Konfiguration implementiert. Geräte erscheinen dann automatisch in der UTM-/Firewall-Benutzeroberfläche, wo sie manuell aktiviert werden können. So erhalten die Vereine einen sicheren, einfach zu bedienenden und sofort einsatzbereiten Gastzugang – ohne zusätzliche Appliances, Lizenzen oder komplizierte Konfiguration.

Die Null muss stehen!

Nicht nur die Keeper der Bundesliga-Vereine müssen ihren Kasten sauber halten, sondern auch IT-Admins auf aller Welt. Während die Sportler dabei „nur" ihre Torwarthandschuhe als technische Helferlein haben, setzen verschiedene Profi-Fußballteams auf das Netzwerk-Sicherheitspaket Sophos UTM mit On-Premise- oder virtueller SG-Appliance. Und damit auch zukünftige Attacken erfolgreich abgewehrt werden können, ist Sophos UTM eines der ersten Sophos-Produkte, mit dem unsere Advanced Next-Gen Cloud Sandboxing Technologie genutzt werden kann. Sophos Sandstorm hebt Advanced Threat Protection auf ein neues Level – mit modernsten Schutz-, Visibility- und Analyse-Funktionen zur Abwehr gezielter Angriffe. Die Technologie erkennt evasive Malware schnell und zuverlässig, bevor diese in Ihr Netzwerk gelangen kann.

Sales DACH (Deutschland, Österreich, Schweiz)
Tel.: +49 611 5858 0 | +49 721 255 16 0
E-Mail: sales@sophos.de

2018-06-12 NA (PS)

SOPHOS