Belsoft infortix

Universität St. Gallen: Endpoint Security aus der Cloud mit Sophos Intercept X

Die Universität St. Gallen vertraut beim Schutz ihrer 250 Applikationsserver seit mehr als 15 Jahren auf Sophos-Produkte und Infortix. Nun entschieden sich die IT-Verantwortlichen für den Wechsel auf eine Cloud-basierte Lösung. Mit Sophos Central Intercept X Advanced for Server verbessert sich der Schutz vor Bedrohungen dank Deep Learning, Machine Learning und der automatischen Isolation von betroffenen Servern.

Universität St.Gallen

Universität St.Gallen

Die Universität St.Gallen (HSG) wurde 1898 als Handelsakademie gegründet und ist heute eine Hochschule für Wirtschafts-, Rechts- und Sozialwissenschaften, Internationale Beziehungen und Informatik. Sie gehört zu den führenden Wirtschaftsuniversitäten in Europa und ist EQUIS-, AACSB- und AMBA-akkreditiert.

Die IT-Abteilung der Universität St. Gallen besteht aus knapp 60 Mitarbeitenden, darunter fünf Lernende und IMS-Praktikanten. Sie ist in die Bereiche IT Applikationsmanagement, IT Backend Services, IT Frontend Services, IT Service Operation und IT Service Management unterteilt.

Dr. Kurt Städler
Leiter IT Backend Services

www.unisg.ch/

Die Belsoft Infortix AG und die Universität St. Gallen verbindet eine langjährige Partnerschaft im Bereich Endpoint Security für Server. Im Jahr 2019 wurde die bestehende Lösung ersetzt.

Die Aufgabenstellung

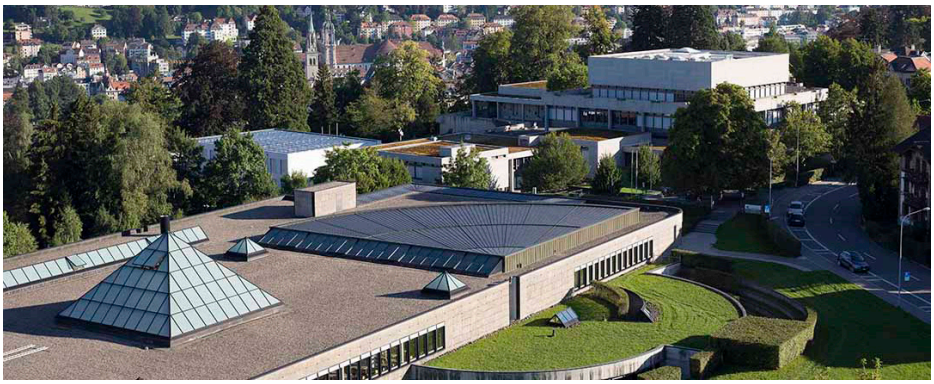
Die Universität St. Gallen setzt bereits seit über 15 Jahren auf Technologien von Sophos, um ihre rund 250 Applikationsserver zu schützen. Als der Lizenzvertrag des bisherigen Produkts Sophos Server Protection auslief, entschieden sich die Verantwortlichen, den Wechsel auf eine Cloud-basierte Managementlösung zu prüfen. Dies war zuvor aufgrund von öffentlichen Vorgaben nicht möglich, weshalb die klassische, signaturbasierte Antivirenlösung im Einsatz war.

«Die Cloud-Version bietet wichtige Funktionalitäten wie intelligente Malware-Detection, die On-Premise nicht verfügbar sind», erklärt Kurt Städler, Leiter IT Backend Services. «Zudem bietet die Cloud natürlich den Vorteil, dass wir weniger Infrastruktur selbst betreiben müssen.» Schnell war aber auch klar, dass weiterhin auf ein Sophos-Produkt gesetzt werden sollte: «Wir sind mit der Software sehr zufrieden und haben uns an die übersichtliche Verwaltung gewöhnt», so Städler.

Als langjähriger Partner für Endpoint-Security führte die Belsoft Infortix AG deshalb zusammen mit Städlers Team einen Proof-of-Concept für Sophos Central Intercept X Advanced for Server durch. Sie prüften, ob das bisherige, etablierte Design auch mit der Cloud-Lösung funktioniert. Nach einem erfolgreichen Test fiel die Entscheidung zugunsten von Intercept X.

Die Lösung

Sophos Central Intercept X Advanced for Server gilt seit Jahren als Spitzenreiter im Bereich Endpoint Security und erhält von den Anwendern regelmässig Bestnoten. Das Programm arbeitet mit Technologien wie Deep Learning und Machine Learning, um die Zuverlässigkeit laufend zu erhöhen und False Positives so gering wie möglich zu halten. Betroffene Server werden automatisch im Netzwerk isoliert, um die



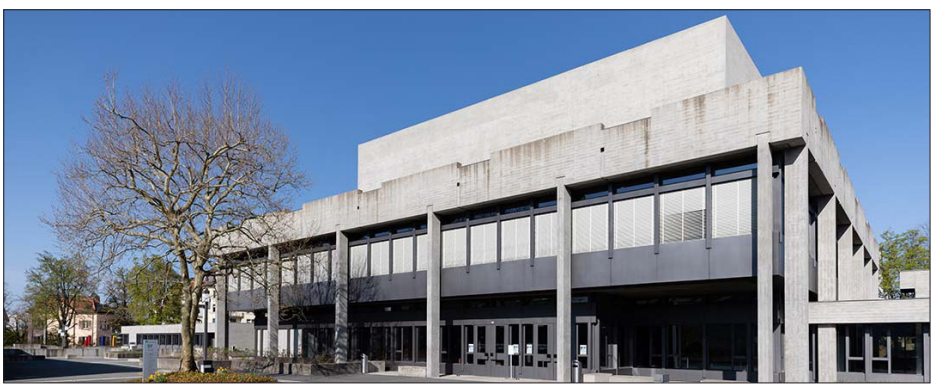
Ausbreitung zu verhindern. Auch Ransomware wird effektiv gestoppt, indem das Programm einen Ausbruch rasch erkennt, unterbindet und bereit verschlüsselte Elemente wiederherstellt – und das alles ohne manuelles Zutun eines Administrators. Die Lösung passt so auch optimal zu den zur Verfügung stehenden Ressourcen der Universität St. Gallen. Auf eine Erweiterung mit Endpoint Detection and Response (EDR) etwa wurde aus Kapazitätsgründen bewusst verzichtet.

Die Einrichtung von Intercept X und der Ersatz der bestehenden Lösung gestalteten sich sehr einfach. Der Austausch der Agenten auf den rund 250 Servern wurde durch einen Migrationspfad von Sophos grösstenteils automatisiert und erforderte kaum manuelle Arbeit. Die Infortix-Experten unter Leitung von Philippe Hirzel übernahmen die Installation und Grundkonfiguration der Software. An einem Schulungstag mit dem internen IT-Team wurden diese besprochen und Empfehlungen anhand von Best-Practice-Beispielen diskutiert. Dank einer Testlizenz konnte die Cloud-Version parallel zur bestehenden On-Premise-Lösung in Betrieb genommen werden, was einen fliessenden Übergang mit einer sauberen Migration ermöglichte.

Der Nutzen

Intercept X verstärkt die Sicherheit für die Applikationsserver der Universität St. Gallen und entlastet die internen Ressourcen durch automatisierte Reaktionen im Angriffsfall. Die intuitive Konsole Sophos Central macht die eigenständige Verwaltung durch das IT-Team einfach möglich. «Man merkt klar, wieso das Produkt im Gartner-Quadrant im Vergleich zur Konkurrenz so stark positioniert ist», lobt auch Kurt Städler.

Die langjährige gute Zusammenarbeit zwischen der Universität und Infortix ermöglicht einen engen Kontakt und eine effiziente Kommunikation mit raschen Rückmeldungen auf Fragen und Probleme. Werden grössere Updates von Intercept X publiziert, so geht Infortix proaktiv auf den Kunden zu, um die Administratoren auf den neusten Stand zu bringen. Diese persönliche Beziehung wird auch von Kurt Städler geschätzt: «Wir sind sehr froh über die grosse Kontinuität, die im Team der Belsoft Infortix AG herrscht.»



Belsoft infortix

Die Belsoft Infortix AG wurde 2014 als Tochtergesellschaft der Belsoft AG gegründet. Die Belsoft AG ist seit 1996 auf dem Schweizer Markt tätig.

Belsoft Infortix AG ist ein eigenständiges IT-Dienstleistungs- und Handelsunternehmen, mit Niederlassungen in Zürich, Pfäffikon SZ und Widnau SG, das sowohl kleine und mittelständische als auch Grossunternehmen mit Dienstleistungen und Fachwissen rund um das Thema Informatik unterstützt.

Die Belsoft Infortix AG ist in drei Bereiche unterteilt:

- Cloud Solutions
- IT-Services
- Enterprise Solutions

Die Abteilung Enterprise Solutions setzt erfolgreich Projekte für ihre Kunden um:

- Datacenter / IT-Infrastruktur
- Server- & Storage-Lösungen
- Backup & Desaster Recovery Lösungen
- Firewalling / Security
- Endpoint Protection
- Endpoint Management
- Wireless & LAN- / WAN-Lösungen