Sicherheitsüberlegungen für das *Digital Signage*

Technische Studie 1.0
von *SpinetiX*

08.2021

Was deckt dieses Dokument ab?

Diese Studie stellt die wesentlichen Aspekte dar, deren sich das technische Personal bewusst sein sollte, um die Sicherheitsrisiken und -anforderungen eines Digital Signage Projektes zu bewerten. Wir empfehlen, dass Sie dieses Dokument als Basis verwenden, um Digital Signage Lösungen mit Ihren IT-Sicherheitsanforderungen abzugleichen. Dieses Dokument ist Teil der Reihe unserer Digital Signage Sicherheitsstudien.

Cybersecurity: Priorität für jeden

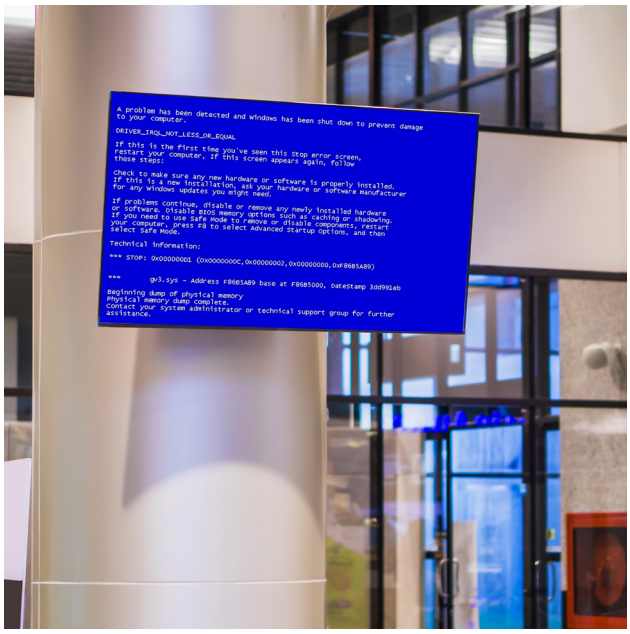
Da unsere Welt jeden Tag digitaler und vernetzter wird, ist die Sicherheit im Netz wichtiger als je zuvor. Die Digital Signage Branche hat im Wesentlichen, wenn man es historisch betrachtet, die angewandten, besten Lösungen zur IT-Sicherheit ignoriert. Der gesunde Menschenverstand sagt einem, dass die Anzahl von Angriffen mit der stärkeren Verbreitung miteinander verbundener Digital Signage Systeme nicht sinken kann. Damit ist es wichtig, Sicherheitsüberlegungen ins Zentrum bei Planung, Implementierung und Betrieb von Digital Signage Lösungen zu stellen.

Bei der Wahl von Produkten für ein neues Projekt stehen Sicherheitsaspekte sehr oft zu Lasten anderer Entscheidungsparameter wie Anschaffungspreis, laufende Kosten, Leistungsmerkmale und genereller Leistung und damit insgesamt eher weniger im Fokus. Zusätzlich kann man es bei Planung und Implementierung von Digital Signage Installationen mit Anspruchsgruppen zu tun haben, die sehr unterschiedliche Ansprüche an die Sicherheit – typischerweise der Marketing- bzw. der EDV-Bereich – stellen. Dies erhöht das Risiko, dass Sicherheitsaspekte nicht entsprechend gewürdigt werden.

Neue Risiken treten permanent auf. Hier sei auf das neue „Ransomware as a Service (Raas)“- Modell hingewiesen, das im Jahr 2021 durch die Revil-Gruppe und die weltweiten Infrastrukturattacken auf Kaseya und andere und seiner neuen „doppelten Erpressungstaktik“ Schlagzeilen machte. Letztere basiert auf der Drohung, bei Nichtzahlung von Geld vertrauliche, gestohlene Informationen allgemein zugänglich zu machen. Es ist daher unabdingbar, dass die Sicherheit eines Produktes nicht nur zum Zeitpunkt des Erwerbs, sondern auch vor dem Hintergrund des allgemeinen Supports und der Verfügbarkeit von Schwachstellenpatches über den Lebenszyklus eines Produktes hinweg beurteilt wird.

Die versteckten Kosten der Sicherheit

Es ist nicht ungewöhnlich, dass Digital Signage Player direkt mit dem Internet verbunden sind, ohne überhaupt mit einem Passwort oder zumindest mit einem Standardpasswort geschützt zu sein. Die meisten der Signage Player funktionieren mit einem ungepatchen oder einem nicht unterstützten Betriebssystem, dessen Schwachstellen entsprechend bekannt sind. Angreifer können so unter Verwendung von Exploit-Kits den vollen Zugang aus der Ferne erreichen. Dessen ungeachtet werden regelmäßige Updates oft als kostspielig und unnötig und daher als etwas, das es besser zu vermeiden gilt, angesehen. Die Sicherheit ist selten ein Aspekt bei der Wahl einer Signage Lösung.

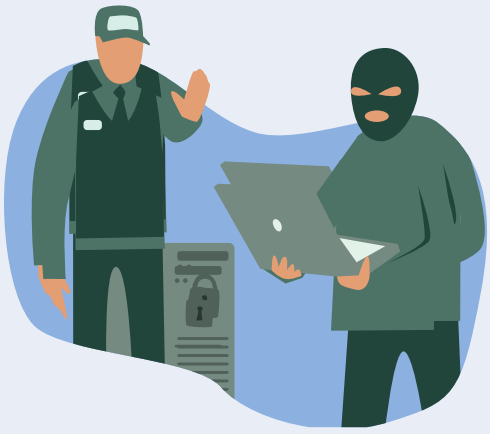


Trotzdem steigen die versteckten Kosten von unsicherer Hard- und Software rasant. Es gibt gut dokumentierte Studien verschiedener Netzwerkanwendungen, mit denen gezielt zu vermietende Botnets geschaffen wurden: Persirai (120.000 beeinträchtigte Systeme) und Mirai (600.000 Systeme).

Um eine Trend Micro Analyse zu zitieren: „In mehreren namhaften und mächtigen DDoS Attacken legte Mirai, eine auf Linux ausgerichtete Software, offen, wie zersplittert das Ökosystem des Internets der Dinge ist. Die Malware macht jetzt dank eines neuen Windows-Trojaners, der seine Vervielfältigungsmöglichkeiten drastisch erhöht hat, wieder Schlagzeilen."

In den letzten Jahren gab es ebenfalls unzählige andere, weniger schlagzeilenträchtige, aber keineswegs weniger schädliche Attacken, die speziell auf Digital Signage Infrastrukturen gerichtet waren. Die Effekte daraus reichen von der relativ harmlosen „Bitte sichern Sie Ihr System!"-Meldung bis hin zu Lösegeldforderungen oder sogar der Projektion von Hardcore-Pornographie im öffentlichen Raum, wie im Washington Union Bahnhof geschehen.

Warum die Sicherheit wichtig ist



Entscheider gehen fälschlicherweise oft davon aus, dass alle Anbieter von Lösungen dasselbe Sicherheitsniveau haben. Damit sei die Wahrscheinlichkeit, dass jemand eine Schwachstelle ausnutzt, vernachlässigbar gering. Alternativ wird angenommen, dass die Auswirkungen von Sicherheitsverletzungen praktisch Null seien. Beide Annahmen erweisen sich in der realen Welt als auf keinen Fall haltbar.

Das Risiko eines Sicherheitsangriffs ist real und nicht ohne Folgen. Ein Verstoß kann Sie Ausfallzeiten, verlorene Werbeeinnahmen und sogar Ihr Firmenimage kosten. Eine kompromittierte Digital Signage Installation kann auch zum Angriff auf andere IT-Infrastrukturen verwendet werden.

Ein häufiges Missverständnis ist, dass eine Software sicher bleiben kann, ohne dass etwas unternommen wird. Jede Software hat unbekannte Sicherheitslücken, auch «zero-day» genannt. Es ist daher wichtig, dass sie, sobald sie bekannt sind, schnell korrigiert werden und dass die Fehlerbehebungen effektiv eingesetzt werden können.

Eine andere, falsche Vorstellung ist, dass Signage Player kein Ziel von Hackern seien. In der Tat ist es so, dass jede Anwendung für einen Hacker ein potenzielles Ziel sein kann, falls sie nicht geschützt ist. Dies ist so, weil sie dazu verwendet werden kann, weitere Zugriffe auf höherwertige Ziele innerhalb des Unternehmensnetzwerkes zu ermöglichen. Ausgefeilte Attacken sind dadurch gekennzeichnet, dass sie immer am schwächsten Eingangspunkt ansetzen. Die „Internet der Dinge» - Anwendungen sind damit ein Ziel erster Wahl. Diese Technik, «laterale Bewegung» genannt, ist im Jahr 2019 eine der wichtigsten Bedrohungen für Unternehmensnetzwerke geworden. Durch sie hat nämlich die Zahl der Zugangspunkte für Ransomware oder Datenlecks im Vergleich zu normalerweise besser geschützten erheblich zugenommen. Trotz der Tatsache, dass automatische Updates üblicher geworden sind, hat der Sunburst Hack des Jahres 2020 die Realität von Supply-Chain-Attacken offengelegt.

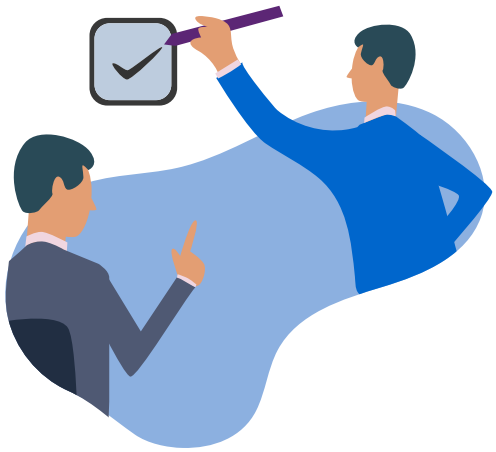
Natürlich gibt es direkte Kosten, die im Zusammenhang mit Sicherheitsausfällen bei den Komponenten einer Digital Signage Lösung entstehen. Beeinträchtigte Player müssen offline gehen. Ihr Ersatz ist teuer. Beeinträchtigte Player oder Nutzerkonten können dazu missbraucht werden, rufschädigende oder illegale Inhalte anzuzeigen. Sie können zu unmittelbaren Umsatzausfüllen im Bereich der Werbung oder Serviceverträgen führen. Falls über sie Ransomware verbreitet wird oder ein Angriff auf hochvertrauliche persönliche Informationen erfolgt, kann das Schadensniveau verheerend sein. Zusätzlich führen kürzlich erfolgte behördliche Änderungen wie das GDPR der EU vor Augen, dass es wichtig ist, Lösungen zu wählen, die die Compliance vereinfachen und die damit verbundenen Kosten senken.

Sicherheits-Checkliste

Was Sie bei der Sicherheitsbewertung einer Digital Signage Einrichtung beachten sollten.

In einem Digital Signage Netzwerk gibt es zahlreiche Punkte, an denen mögliche Schwachstellen zu berücksichtigen sind. Am sichtbarsten und am einfachsten zu bewerten ist die physische Sicherheit am Bildschirmstandort, falls sich dieser an einem öffentlichen oder sensiblen Ort befindet. Viel schwieriger zu beurteilen sind die Sicherheit des Digital Signage Players, die Sicherheit des Displays selbst, die der Netzwerkanbindung und des Netzwerks selbst, in dem der Player installiert ist.

Hinzu kommen die Sicherheit der Inhaltsakquisition, des Vertriebs und der Produktion, die ebenfalls bewertet werden müssen. Und schließlich, wie man sicherstellt, dass Betreiber gute Sicherheitsrichtlinien befolgen. All diese Punkte sollten bei der Produktauswahl und der Planung für Digital Signage von Anfang an berücksichtigt werden. Das Hinzufügen von Sicherheit im Nachhinein kann unmöglich oder sehr kostspielig sein, sobald Sie an ein Produkt gebunden sind. Der Preis für Sicherheit in Digital Signage.



Die Bewertung der Sicherheit eines Systems ist ein herausforderndes Problem, aber es gibt einige grundlegende Fragen, mit denen Sie sicherstellen können, dass die ausgewählten Produkte den Sicherheitsrichtlinien entsprechen.

Verwenden Sie die unten aufgeführte Checkliste als Hilfestellung, um Ihr bestehendes Netzwerk bzw. Ihre Prozesse zu bewerten. Gleiches gilt für die Auswahl Ihrer zukünftigen Digital Signage Lösungen

AUF DER SEITE DES ANBIETERS:

Die Antworten auf die unten aufgeführten Punkte zeigen Ihnen, ob Sie sich auf den Anbieter stützen können, was die korrekte Wartung seiner Produkte von einem Sicherheitsstandpunkt aus angeht.

- [ ] Ist der Lösungsanbieter gut etabliert? Haben sie eine gute Erfolgsbilanz?
- [ ] Werden regelmäßige Sicherheitsupdates nach termingerechten Vorgaben bereitgestellt?
- [ ] Wie lange wird das ausgewählte Produkt gewartet?
- [ ] Verfügen sie über einen Arbeitsprozess zur Offenlegung von Schwachstellen, zum Beispiel mit der CVE-Liste?
- [ ] Verfügen sie über einen klar definierten Veröffentlichungsprozess, einschließlich Versionshinweisen mit einer Liste der im Update behobenen Sicherheitsprobleme?
- [ ] Wie werden Updates verteilt und wie teuer ist die Bereitstellung?
- [ ] Wie ist die Kompatibilität mit früheren Versionen von Updates?
- [ ] Gibt es einen fähigen Support Service, den Sie gut erreichen können?

AUF DER LÖSUNGSSEITE:

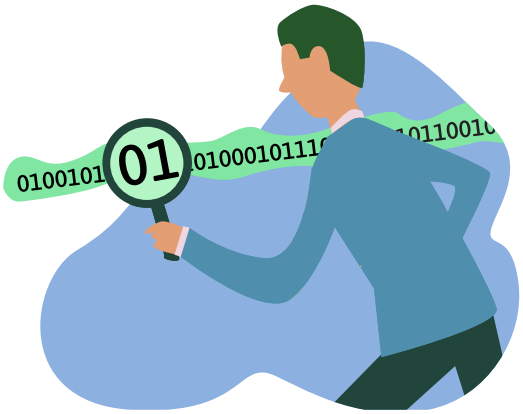
Verwenden Sie die unten aufgeführte Checkliste als Hilfestellung, um Ihr bestehendes Netzwerk bzw. Ihre Prozesse zu bewerten. Gleiches gilt für die Auswahl Ihrer zukünftigen Digital Signage Lösungen.

- ☐ Der Inhalt auf dem Bildschirm stimmt mit dem geplanten Inhalt überein.
  - ☐ Vermeiden Sie die Verbreitung von bösartigen, illegalen oder heimtückischen Inhalten durch Eindringlinge oder Insider und dem daraus resultierenden Imageschaden des Anbieters.
  - ☐ Vermeiden Sie Umsatzverluste, falls die verkaufte Werbung nicht zum vereinbarten Zeitpunkt und am vereinbarten Ort gezeigt wird.
  - ☐ Aktuelle Inhalte sind flexibel verfügbar, so dass ihre zeitgerechte Verteilung gesichert ist.
- ☐ Der Media-Player sollte keine Bedrohung für die Sicherheit anderer Ausrüstungsbestandteile im Netzwerk darstellen. Er stellt keinen Schwachpunkt für Attacken dar, die zum Stehlen von Daten oder der Verbreitung von Malware, Spyware oder Ransomware ausgenutzt werden können.
- ☐ Schutz von Kundendaten auf dem Player oder in der Cloud vor dem Zugang von nicht autorisierten Drittparteien. Falls eine Sicherheitsübertretung oder ein Datenmissbrauch stattfindet, stehen Instrumente für eine juristische Analyse zur Verfügung.
- ☐ Integriert sich nahtlos in die hauseigene EDV-Politik des Kunden zum Schutz des Host-Netzwerkes unter Unterstützung unternehmensinterner Abläufe.
- ☐ Erleichtert die Compliance mit gesetzlichen Verpflichtungen, z. B der Implementierung der GDPR-Direktive in der EU oder der CCPA/CPRA in den USA.

Der Preis für Sicherheit.

All dies hat seinen Preis, und es sollte nicht überraschend sein, dass eine sichere Lösung kostspieliger ist, obgleich das Gegenteil natürlich nicht stimmt. Sichere Systeme zu entwickeln ist schwierig und trägt daher zusätzliche Kosten mit sich. Eine sichere Plattform aufrechtzuerhalten, wenn Schwachstellen entdeckt werden, ist zeitaufwendig und verursacht zusätzliche Kosten.

Sobald Sie einen Anbieter ausgewählt haben, der Ihren Sicherheitsanforderungen entspricht, sollten Sie auch solide Sicherheitsprinzipien für die Bereitstellung und den Betrieb anwenden. Verringern Sie die Angriffsfläche so weit wie möglich, indem Sie unnötige Dienste deaktivieren und die Bereitstellung der Dienste im Netzwerk einzig auf die für die Anwendungen notwendigen begrenzen. Verbinden Sie Ihre Geräte nicht direkt mit dem Internet aus und verwenden Sie eine Firewall, um das Netzwerk des Players zu schützen. Stellen Sie sicher, dass die Benutzer ausreichend geschult sind, um nicht Opfer von Social Engineering Angriffen zu werden und, dass sie sichere und individuelle Passwörter verwenden.



Das Fazit.

Hie gib es augenscheinlich eine Menge zu bedenken, aber wenn die richtigen sicherheitsrelevanten Fragen von Beginn eines Projekts an berücksichtigt und die Sicherheitsaspekte in den Auswahlprozess integriert werden, sollte es nicht so schwierig sein, die richtigen Produkte auszu- wählen, die das Risiko, Opfer eines erfolgreichen Angriffs zu werden, vermindern.

Ein paar Worte über den Autoren.

Jean-Claude Michelou,
Vice President Forschung und Entwicklung

Jean-Claude bringt seine Erfahrungen in der Entwicklung großformatiger Netzwerkinfrastrukturen und komplexer Technologieprojekte bei SpinetiX ein. Er leitet die Firma im Bereich Entwicklung und somit bei der Schaffung bahnbrechender Produkte.

Nach der Absolvierung der Ecole Polytechnique in Paris (X94) hatte Jean-Claude mehrere Forschungs- und Ingenieurposten in Silicon-Valley Start-ups wie AltaVista und BigVine inne. Dann war er der Mitgründer von VisioWave, wo er als Vice President für Forschung und Entwicklung und hauptverantwortlicher Softwareentwickler die Videostreamingtechnologie entwickelte, die heute hunderte öffentlicher Transportverkehrssysteme weltweit sichert.

Diego Santa Cruz, PhD
Technologiearchitekt bei SpinetiX

Diego ist seit über 10 Jahren leidenschaftlicher Experte für die Sicherheit von SpinetiX Produkten und bemüht sich um die Lieferung von sicheren, zuverlässigen und gut integrierten Produkten. Er war Mitbegründer von SpinetiX und ist im Unternehmen für die Entwicklung der Systemebene verantwortlich.

Diegos Hauptkompetenzen umfassen die System- und Kernelentwicklung, Netzwerkprotokolle, Sicherheit, IT und Elektronik sowie auch Bild- und Videosysteme, wo er auch promoviert hat. Als Autor mehrerer Patente und früher Linux Anwender, war Diego ein Mitwirkender in den JPEG- und MPEG-Ausschüssen.

SPINETIX™
N°1 IN DIGITAL SIGNAGE SOLUTIONS

Machen Sie Ihre ersten Schritte in Digital-Signage?

Brauchen Sie Ratschläge im Bereich Sicherheit?

Kontaktieren Sie uns:

sales@spinetix.com

Lesen Sie weitere Publikationen aus unserer Reihe über Sicherheit:

spinetix.com/security