

PRESSEMITTEILUNG

Zur sofortigen Veröffentlichung freigegeben.
Abdruck honorarfrei, Belegexemplar erbeten.

Gegen Angriffe aus dem eigenen Browser: Sevenval erhält EFRE-Förderung für die Entwicklung neuer Internet-Sicherheits-Technologien

Die Investitionsbank Berlin fördert die Forschung an neuen Sicherheits-Technologien für Internet-Nutzer aus Mitteln des Europäischen Fonds für regionale Entwicklung (EFRE). Sevenval erhält den Auftrag, eine neue Schutzlösung zu entwickeln, um die Nutzung des Internet für alle Nutzer sicherer zu machen. Das Forschungsprojekt heißt „Web Security Optimizer“.

Berlin & Köln, 17.07.2017 – Mit der zunehmenden Digitalisierung immer weiterer Lebensbereiche steigt das Bedürfnis nach Sicherheit im Internet bei Bürgern und Unternehmen. Denn mit der schnellen technologischen Entwicklung einher geht auch eine weite Verbreitung kritischer Schadsoftware, die Nutzer und Anbieter gefährdet und zu hohen finanziellen Schäden führt. Das Land Berlin fördert deshalb die Entwicklung neuer Sicherheits-Technologien durch die Sevenval Technologies GmbH mit Mitteln aus dem Europäischen Fonds für regionale Entwicklung (EFRE). Die finanzielle Unterstützung für das Forschungsvorhaben wird von der Investitionsbank Berlin (IBB) bereitgestellt.

Für das „Internet Labor“ von Sevenval Technologies ist es bereits der zweite geförderte Forschungsauftrag. Das Unternehmen entwickelt seit 1999 Web- und Frontend-Technologien. Die Sicherheits-Experten haben sich zum Ziel gesetzt, einen „Web Security Optimizer“ zu entwickeln, der potentielle Gefahren für Nutzer und Betreiber von Web-Angeboten ohne aufwändige Einrichtung erkennt und ausschaltet. Der Forschungsaufwand dabei ist hoch: Die Entwickler gehen ins Rennen mit sich schnell weiterentwickelnder Web- und Browser-Technologie sowie Programmierern von Schadsoftware.

"Unser Ansatz stellt die Sicherheit der Anwender, also der normalen Internetnutzer, in den Vordergrund", sagt Roland Guelle, als CTO von Sevenval verantwortlich für Forschung und Entwicklung. „Neue Web-Technologien eröffnen auch neue Angriffsvektoren für Malware auf die User, etwa direkt aus dem eigenen Browser heraus. Heute ist die gut abgesicherte Website im Rechenzentrum deshalb nur noch ein Baustein für eine insgesamt sichere Web-Anwendung. Zunehmend entscheidend ist die Sicherheit beim Nutzer.“

Malware – ein Problem für Anbieter und Nutzer

Über 600 Millionen Schadprogramme sind aktuell bekannt, die meisten davon für Windows-Betriebssysteme, aber auch bei Mobilgeräten und Macs steigt die Zahl deutlich an. Einen wachsenden Anteil daran hat so genannte „Ransomware“, Erpressungs-Software, wie etwa

„WannaCry“, das in diesem Jahr viel Schaden anrichtete und über Berichterstattung in den Medien sehr bekannt wurde. Schon seit Jahren eine hohe Verbreitung findet aber Malware, die weniger in der öffentlichen Wahrnehmung steht, weil sie Nutzern nicht direkt erkennbar schadet: Browser-Erweiterungen, die einen Mehrwert versprechen aber im Hintergrund das Surf-Verhalten überwachen, kostenlose Spiele, die eigentlich nur Werbung verteilen – das Spektrum ist breit und viele Nutzer merken gar nicht, dass sie Malware auf ihrem Gerät installiert haben.

Ein relevantes Beispiel dafür ist die weit verbreitete aber teils noch unbekannte „Client Side Ad Injection“: Ein Browser-Plugin oder eine Malware, vom Nutzer ohne Kenntnis der Sicherheitsrisiken installiert, lädt im Hintergrund so genannte „Injection Libraries“ in den Browser nach. Über diese wird zum Beispiel Werbung ausgeliefert, die sich über Webseiten legt, die der Nutzer ansteuert. Der Anbieter der Website merkt davon nichts, weil der gesamte Prozess beim „Client“ stattfindet. Die Werbebanner und die Libraries werden von Werbe-Netzwerken bereitgestellt, die für jede Einblendung oder für jeden Klick vom Unternehmen hinter der Werbung bezahlt werden. Der Nutzer muss im Extremfall jede Menge Banner und Popups schließen, bevor er die Seite sehen kann, die er aufgerufen hat. So finanzieren seriöse Anbieter von Waren oder Dienstleistungen über ihre Marketingbudgets unbewusst und ungewollt die Verteilung von Malware an Endkunden.

Es gibt weitere Anwendungsfälle und es werden mehr. Basierend auf dem Ansatz, direkt im Browser des Nutzers Content auszutauschen oder über angesteuerte Webseiten zu legen, können auch „echte“ Klick-Aktionen eines Nutzers ausgelöst werden, durch die beispielsweise persönliche Daten übermittelt oder die Kamera des Laptops für Dritte freigegeben wird. Mit steigender Komplexität wachsen hier die Möglichkeiten – für Anbieter und Nutzer, aber eben auch für Kriminelle.

Forschung für mehr und einfachere Sicherheit

Um die Situation für Nutzer und Unternehmen zu verbessern, entwickelt Sevenval deshalb einen „Web Security Optimizer“. Eine zentrale Annahme der Sicherheitsforscher ist dabei, dass die Sicherheit von Webseiten nicht mehr alleine durch IT-Infrastruktur und die Einhaltung bestimmter Sicherheitsstandards auf Seiten der Anbieter verbessert werden kann, sondern nur durch die Betrachtung der gesamten Kette. Und dazu gehören auch Daten-Transport, Web-Technologien und der Browser des Nutzers. Gerade das Web-Frontend ist demnach für den Endanwender sicherheitsrelevant. Der „Web Security Optimizer“ soll deshalb alle Maßnahmen zur Erkennung und Sicherung der Frontend-Infrastruktur in einem Sicherheits-Layer bündeln.

Diese „Sicherheitsschicht“ soll zwischen den Anbieter (Server) und den Nutzer (Client) nach Art eines Content Delivery Networks (CDN) geschaltet werden. Das ermöglicht Maßnahmen zur Erhöhung der Sicherheit der Nutzer, ohne aufwendig auf Server oder Client eingreifen zu müssen. Und das funktioniert auch nachträglich: Bestehende Webseiten, die nicht mehr aktuellen Standards entsprechen, können ihren Nutzern so die nötige Sicherheit bieten.

Weitere Informationen zum Stand der Forschung am „Web Security Optimizer“ wird Sevenval in den nächsten Monaten veröffentlichen. Achten Sie auf unseren Blog (sevenval.com/blog) und unseren Twitter-Account ([@sevenval](https://twitter.com/sevenval)) oder wenden Sie sich an unsere Pressestelle.

Über den Zitatgeber Roland Guelle:

Roland Guelle ist als CTO der 1999 gegründeten Sevenval Technologies GmbH verantwortlich für Forschung und Entwicklung. Mit 150 Mitarbeitern in Köln und Berlin hat sich Sevenval auf Frontend-Lösungen spezialisiert, die eine moderne, schnelle und vor allem sichere User Experience auch auf Basis historisch gewachsener IT-Systemlandschaften ermöglichen.

Der dreifache Vater Roland Guelle (*1976) ist seit 2001 bei Sevenval. Davor war er mehrere Jahre als Software-Entwickler für verschiedene Unternehmen tätig. Roland entwickelt auch heute noch selbst, spricht regelmäßig auf Entwickler-Konferenzen und twittert als [@rolandguelle](https://twitter.com/rolandguelle) über Technologie und Nerdiges aus dem Web.

Ansprechpartner Sevenval:

Christian Brand

Pressesprecher

Sevenval Technologies GmbH

Bahnhofsvorplatz 1

50667 Köln

christian.brand@sevenval.com

+49 221 84630 -460

Sevenval Technologies GmbH

Seit 1999 entwickelt und implementiert Sevenval mit eigener Technologie und UX-Kompetenz branchenspezifische Frontend-Lösungen. Das Kölner Unternehmen ermöglicht seinen Kunden dabei eine reibungslose Kompatibilität mit bestehenden IT-Systemlandschaften und bietet zugleich den Endnutzern eine optimale User Experience. Auf das konzeptionelle Know-How und die Umsetzungsstärke der "Frontend-Experten" setzen Konzerne wie Allianz, Bosch, Douglas, Frankfurter Allgemeine Zeitung, HDI und Mercedes-Benz. Sevenval hat rund 150 Mitarbeiter, sitzt in Köln und betreibt eine Niederlassung in Berlin.

Sevenval. Wir wissen wie. Frontend-Experten seit 1999.

Weitere Informationen: www.sevenval.com



Europäischer Fonds für regionale Entwicklung

Der Europäische Fonds für regionale Entwicklung (EFRE) ist das wichtigste Instrument der Regionalförderung der Europäischen Union. Er trägt zu den Maßnahmen bei, die den wirtschaftlichen und sozialen Zusammenhalt der Europäischen Gemeinschaft durch Ausgleich der wichtigsten regionalen Ungleichgewichte stärken. Zu diesem Zweck werden die Regionalwirtschaften entwickelt und strukturell angepasst und die grenzübergreifende, interregionale und transnationale Zusammenarbeit gefördert. Der EFRE zielt dabei insbesondere auf die Notwendigkeit ab, Wettbewerbsfähigkeit und Innovation zu stärken, dauerhafte Arbeitsplätze zu schaffen und zu erhalten, sowie eine nachhaltige Entwicklung zu gewährleisten. Weitere Informationen: ec.europa.eu/regional_policy/de/funding/erdf/

Investitionsbank Berlin

Die Investitionsbank Berlin ist die Förderbank des Landes Berlin mit den Geschäftsfeldern Wirtschafts- und Immobilienförderung. In der Wirtschaftsförderung verfügt die IBB über ein breites Programmangebot mit Darlehen, Beteiligungen und Zuschüssen zur Förderung von Gründungsvorhaben, Wachstumsinvestitionen und technologischen Innovationen. Im Geschäftsjahr 2016 erteilte die IBB in der Wirtschaftsförderung Finanzierungszusagen im Volumen von 281 Mio. Euro zur Förderung von rund 1.000 Unternehmen in der Hauptstadt. Von diesen Zusagen entfielen rund 74 Mio. Euro auf Zuschüsse und 207 Mio. Euro auf Darlehen und Beteiligungen.

Weitere Informationen: www.ibb.de



EUROPÄISCHE UNION

Europäischer Fonds für regionale Entwicklung

