E-Commerce-Security

entwickler.de – entwickler.de Deine Wissensplattform

[…]Weiterlesen…
von Steffen Ritter

Eine Forsa-Umfrage [1] zeigt: Über 70 Prozent der Unternehmen sehen sich nicht durch Cyberkriminelle gefährdet. Gerade das E-Commerce-Umfeld ist für Kriminelle jedoch besonders interessant – und damit einem hohen Risiko ausgesetzt. Aber wie erkennen Betreiber Handlungsbedarf, wie stellen sie sich am besten auf – und wieso ist IT-Security nicht nur ein technisches, sondern auch ein betriebswirtschaftliches Thema?

Ein E-Commerce-Projekt ins Leben rufen – nie war das einfacher als heute. Eine Fülle freier wie kommerzieller Software und vielfältige Hosted-SaaS-Lösungen, Onlinemarktplätze und Zahlungsdienstleister machen es möglich. Hinzu kommt das breite Angebot an freien Entwicklern, E-Commerce-Dienstleistern und Dokumentationsressourcen für die Umsetzung in Eigenregie. Segen auf der einen und Fluch auf der anderen Seite, denn: Mit diesem Boom sind die Webportale vermehrt auch in den Fokus von Cyberkriminellen geraten. Fast täglich gibt es Meldungen über gehackte Onlineshops, und sowohl das Bundeskriminalamt (BKA) als auch private Studien stellen fest: Cybercrime nimmt drastisch zu. Was viele nicht bedenken, ist, dass nicht nur klassische Onlineshops von diesen Risiken betroffen sind. Bei solchen Angriffen geht es vor allem um den Diebstahl von persönlichen Daten. Daher sind auch immer komplexer werdende Webapplikationen mit umfangreichen geschlossenen Bereichen für Kunden, Mitglieder oder Partner beliebtes Ziel von Angriffen. Denn auch solche Lösungen müssen, um ihre Zwecke zu erfüllen, einen entsprechenden

Umfang an persönlichen Daten speichern.

Laut einer Forsa-Umfrage im Auftrag des Gesamtverbands der Deutschen Versicherungswirtschaft e. V. (GDV) im April 2020 bei kleinen und mittleren Unternehmen sind zwar knapp 70 Prozent der befragten Unternehmen der Meinung, dass das Risiko, Opfer einer solchen Attacke zu werden, in Deutschland hoch ist. Erstaunlicherweise sind jedoch ebenso über 70 Prozent der Befragten der Meinung, dass es sie nicht treffen wird, weil sie zu klein oder zu uninteressant sind. Gerade diese Sorglosigkeit ist leichtsinnig. Betreiber von Webplattformen aller Art sollten sich der Auswirkungen bewusst sein, die sowohl erfolgreiche als auch nicht erfolgreich abgeschlossene Angriffe auf das eigene Geschäft haben können. Mit diesem Wissen können sie die richtigen Maßnahmen ergreifen, um sich und ihre Kunden zu schützen, ohne dabei tiefergehendes Technologie-Know-how zu benötigen.

https://phpconference.com/session-qualification/ipc-php/?layout=contentareafeed&widgetversion=1&utmtrackerversion=1&seriesId=vRYNCmGQh2xZuzqrE

Mögliche Folgen eines Cyberangriffs

H**ohe Kosten:** Die aktuelle Rechtslage verpflichtet Unternehmen in vielen Fällen, Cybersecurityvorfälle zu melden. Eine IT-forensische Untersuchung des Vorfalls durch entsprechende Sachverständige ist häufig nicht abzuwenden und mit Kosten für das Unternehmen verbunden. Kam es beispielsweise zu Datenverlust personenbezogener Daten, müssen alle Betroffenen informiert werden. Je nach Größe des Unternehmens und Auswirkungen des Sicherheitsvorfalls können so weitere Kosten für Marketingmaßnahmen oder Krisenkommunikation entstehen.

Umsatzverlust: Ein Hack wirkt sich oft direkt auf den Umsatz aus. Das beginnt schon damit, dass ein Onlineshop durch einen Angriff gegebenenfalls nicht mehr erreichbar oder voll funktional ist. Auch kann es sein, dass er wegen forensischer

Untersuchungen abgeschaltet werden muss. Doch das ist noch nicht alles: Durch Zugriffsmöglichkeiten auf die Interna könnten Angreifer beispielsweise Bestellungen, Preise oder den Zahlungsstatus manipulieren. Das verursacht Verzögerungen im Betriebsablauf durch notwendige Kontroll- und Korrekturarbeiten nach Inkonsistenzen der Daten, zum Beispiel zwischen Onlineplattform und Lager oder Enterprise-Resource-Planning-(ERP-)System . Im Ergebnis kommt es zu Lieferschwierigkeiten bei „echten Kunden“ – und das führt am Ende zu Unzufriedenheit und Vertrauensverlust beim Kunden sowie weiterem Umsatzverlust.

Imageschaden: Vielleicht noch bedeutender als direkt messbare Umsatzverluste ist die langfristige Schädigung der Kundenbeziehung. Selbst wenn der Angriff keine direkten finanziellen oder persönlichen Auswirkungen auf die Kunden hatte, erschüttert er das Vertrauen in den Betreiber und seine Plattform – und beeinflusst somit die Kundenbindung. Besonders gravierend ist die Lage, wenn sensible Daten gestohlen wurden – seien sie persönlicher Natur oder Kreditkartendaten. Bei der großen Auswahl an Shops und Dienstleistern im Internet und dem damit verbundenen Tiefpreisgefüge ist die Wahl am Ende häufig eine Sympathieentscheidung – eine negative Sicherheitshistorie ist also massiv geschäftsschädigend. Einige Hackerangriffe zielen sogar genau darauf ab. Beim sogenannten Defacing werden Websiteinhalte mit Fehlinformationen manipuliert, um Anbieter zu diffamieren oder sie in juristische Schwierigkeiten zu bringen.

Zivilrechtliche Konsequenzen

Schadenersatzansprüche: Ein Schadenersatzanspruch (vgl. § 823 BGB [2]) in Deutschland ergibt sich aus der Vorsätzlichkeit oder der Fahrlässigkeit einer Handlung, die mittelbar zum Schaden eines Dritten führt. Gemäß IT-Sicherheitsgesetz aus Juli 2015 [3] sind Betreiber von Onlinepräsenzen dazu verpflichtet, alle technisch möglichen

und wirtschaftlich zumutbaren Anstrengungen technischer wie organisatorischer Art zu unternehmen, um ihre Plattformen gegenüber Angriffen zu sichern (vgl. § 13 TMG Abs. 7 [4]). Gemäß Rechtsprechung handelt grob fahrlässig, wer seinen Sorgfaltspflichten in besonderem Maße nicht nachkommt. Die IT-Security-Studie 2019 von eco – Verband der Internetwirtschaft e. V. [5] hat aufgezeigt, dass 72 Prozent der Webdienste kleiner und mittlerer Unternehmen nicht sicher konfiguriert sind. Eine ordentliche und sichere Konfiguration ist aber im Rahmen der technischen Möglichkeiten und auch wirtschaftlich zumutbar.

Dies impliziert in den meisten Fällen eine Schadenshaftungspflicht für den Plattformbetreiber, was auch im Versicherungskontext relevant ist, denn viele Versicherungen schließen grobe Fahrlässigkeit von ihrer Leistungspflicht aus. Üblicherweise sind Schadenersatzforderungen von Kreditkartenunternehmen bzw. Zahlungsanbietern zu erwarten, wenn Daten abhandengekommen sind, die Zahlungsmittelmissbrauch erlauben, sowie von vertraglichen Partnerunternehmen wie Lieferanten, Versanddienstleistern, Hostingpartnern oder Markeninhabern, wenn diesen durch den Angriff Schäden entstanden sind.

Unterlassungsansprüche und Abmahnungen: Wenn ein Betreiber mit seiner Webpräsenz gegen rechtliche Bestimmungen verstößt oder Schutzrechte Dritter verletzt, haben Betroffene das Recht, ihn darauf aufmerksam zu machen und Unterlassung zu fordern – allgemein als Abmahnung bekannt. Das Gesetz gegen unlauteren Wettbewerb [6] definiert Verstöße gegen Rechtsvorschriften als unlauter, was Marktteilnehmern regelmäßig das Recht zur Abmahnung einräumt.

Ein Unterlassungsanspruch dürfte sich also unter den gleichen Maßgaben ergeben wie im Bereich Schadenersatz. Hinzu kommen die möglichen Verletzungen weiterer Ansprüche, beispielsweise durch das Gesetz gegen unlauteren Wettbewerb (UWG), Telemediengesetz (TMG) [7], die Datenschutz-Grundverordnung

(DSGVO) [8], Preisangabenverordnung (PAngV) [9], das Urheberrechtsgesetz (UrhG) [10] und weitere, wenn die Angreifer die Inhalte der Webseite dahingehend bewusst verändert haben.

Vertragsstrafen: Lieferanten, Versanddienstleister, IT-Dienstleister, Hostingprovider, Markeninhaber oder Zahlungsdienstanbieter – Partner und Dienstleister sind in den meisten Fällen essenziell für das Geschäftsmodell hinter der Onlineplattform. Sind diese durch einen Angriff auf ein Portal ebenso beeinflusst worden, kann dies neben den Schadenersatzansprüchen auch zu Vertragsstrafen führen – oder zur Auflösung der Zusammenarbeit.

Bußgelder und Ordnungsgelder: Die beiden wohl bekanntesten Gesetze/Verordnungen im Bereich Web sind die DSVGO und das TMG.

- *DSGVO – Datenschutz-Grundverordnung*: Seit 2018 gilt europaweit die Datenschutz-Grundverordnung der Europäischen Union, die die besondere Schutzbedürftigkeit im Umgang von personenbezogenen Daten regelt. Als Shopbetreiber ist es unausweichlich, während des Bestellprozesses personenbezogene Daten zu erfassen. Werden diese aber missbräuchlich verwendet, etwa weil ein unzureichender Schutz besteht, ist ein Bußgeld in Höhe von bis zu 4 Prozent des Jahresumsatzes zu erwarten.
- *TMG – Telemediengesetz*: Im Telemediengesetz sind beispielsweise die Impressumspflicht oder Bestimmungen gegen Spam geregelt, aber eben auch die Pflicht, zumutbare Anstrengungen zu unternehmen, sein Angebot sicher zu betreiben. Eine Zuwiderhandlung ist als Ordnungswidrigkeit eingestuft, die mit einem Ordnungsgeld in Höhe von bis zu 50 000 Euro geahndet werden kann (vgl. § 16 TMG).

Nachgelagerte Angriffe: Die Dunkelziffer der nicht erkannten Hacks wird auf schwindelerregende Höhen geschätzt. In vielen Fällen ist ein Webportal gar nicht das primäre Ziel des Angriffs und der Angriff nur die erste Stufe eines mehrphasigen Plans. Mit den gewonnenen Daten wie zum Beispiel Benutzernamen/Passwörtern (Mitarbeiter verwenden häufig dieselben Log-in-Daten bei verschiedenen Systemen), internen Dokumenten, Anbindungen an interne Systeme wie ERP, Warenwirtschaft o. ä. werden Angriffe auf weitere Bereiche interner Netzwerke überhaupt erst ermöglicht oder bieten die Grundlage für Spear-Phishing-Attacken mittels Social Engineering.

Wie lässt sich ein E-Commerce-Projekt sicher umsetzen?

Wenngleich die möglichen Risiken abschreckend klingen mögen, so ist es mit entsprechender Sorgfalt kein Problem, sich in diesem Bereich geschäftlich, juristisch wie technisch sicher zu betätigen. Millionen von erfolgreichen und sicheren Webdiensten zeigen dies ganz klar: Mit Vorbereitung, Weitblick und verantwortungsvollem Umgang mit der Thematik lässt sich das Risiko drastisch minimieren und die juristischen Folgen lassen sich reduzieren.

Schritt 1: Überblick über Risiken, Gefahren und Status quo schaffen: Über welche Daten verfügt ein Shop oder Webportal, wo sind Schwachstellen, wen könnte ein Angriff betreffen und welche Pflichten hat der Betreiber? Eine Übersicht bezogen auf das konkrete Projekt hilft, Schwachstellen, Risiken und Handlungsbedarf zu erkennen und Maßnahmen einzuleiten. Eine Dokumentation der Systemlandschaft unter Sicherheitsaspekten und eine Schulung des Teams kann oft einen großen Teil der Risiken kontrollierbar machen. Viele Angriffsvektoren werden dabei auch ohne identifizierbaren Handlungsbedarf erfasst, dafür wird allen Beteiligten vor Augen geführt, was für den

zukünftigen Betrieb, aber auch die Weiterentwicklung hilfreich ist.

Folgende Fragestellungen helfen E-Commerce-Betreibern dabei, einzuordnen, wie sie hinsichtlich Security aktuell aufgestellt sind und wo Handlungsbedarf besteht:

- Werden bei unserem Dienst regelmäßige Updates durchgeführt? Wer führt diese in welchen Intervallen durch? Bestehen Wartungsverträge und Service Level Agreements (SLAs)?
- Wie ist die Lösung gehostet? Welche SLAs liegen dort vor und welche Vereinbarungen existieren dort für Sicherheitsupdates, Back-ups und Ähnliches?
- Teilt sich unsere Plattform einen Server mit anderen Projekten (intern im Haus oder auch extern im Sinne von Shared Hosting)?
- Ist unser Portal mit automatischen Schnittstellen an andere Dienste angebunden, egal ob eingehend oder ausgehend, und wurde diese Verbindung unter IT-Sicherheitsaspekten geplant und umgesetzt? Sind die Datenquellen vertrauenswürdig oder können sie manipuliert werden?
- Habe ich das Gefühl, dass meine Mitarbeiter/Kollegen wie auch beauftragte Dienstleister sich der Sicherheitsrisiken, Abwehrmaßnahmen und Folgen bewusst sind (Security Awareness) und sich regelmäßig weiterbilden?
- Ist aus einem Provisorium eine Dauerlösung geworden oder eine längst abgekündigte Lösung nicht ersetzt worden?
- Wurden Änderungen oder Erweiterungen kurzfristig bis überstürzt umgesetzt, um zum Beispiel einen Produktlaunch zu unterstützen oder dem unerwarteten Ansturm aufgrund einer Marketingmaßnahme gerecht zu werden?

Darüber hinaus können sowohl E-Commerce- als auch Cybersecurityexperten ein Projekt technologisch analysieren und schnell einschätzen, wo es steht – und dann entsprechende Handlungsempfehlungen aussprechen oder selbst handeln. Hier seien exemplarisch die beiden großen Verfahren des Penetrationstests (als Black-Box-Test), aber auch das Begutachten der eingesetzten Komponenten, von Architekturkonzepten und Implementierungen (White-Box-Test) genannt.

Schritt 2: Juristische Beratung: Es empfiehlt sich generell eine juristische Beratung, die branchen- und dienstleistungsspezifisch aufzeigt, welche Gesetze, Verordnungen und berufsrechtliche Regularien im konkreten Tätigkeitsbereich anzuwenden sind und welche konkreten Anforderungen sich daraus für ein Onlineangebot ergeben. Diese Anforderungen kann ein Technologiedienstleister dann in der Entwicklung berücksichtigen. Es ist wichtig zu verstehen, dass der Betreiber selbst dafür verantwortlich ist, dass sein Onlineangebot rechtskonform umgesetzt wird – und selbstverständlich auch über die ganze Lebensspanne des Angebots konform bleibt. Dies muss auch sich verändernde Inhalte oder Rechtslagen berücksichtigen. Der Technologiedienstleister ist (meist) allein für die Umsetzung zuständig und kann weder eine juristische Beratung durchführen noch für die Rechtssicherheit eines Onlineangebots haften.

Schritt 3: Wahl der passenden Dienstleister: Im Optimalfall kennen Technologiepartner und Dienstleister die Risiken und Aspekte der IT-Sicherheit und beziehen diese bereits von der Planung an in Projekte ein. Nicht immer liegt dieses Themenfeld jedoch in der Expertise der Dienstleister. E-Commerce- und Cybersecurityspezialisten können in diesem Fall potenzielle Schwachstellen oder Handlungsbedarf an bestehenden Projekten identifizieren oder in Form von Beratung den Dienstleister wie Anbieter unterstützen.

Zu Beginn eines E-Commerce-Projekts oder eines Relaunchs

bietet es sich an, Security by Design einzuführen und in der Ausschreibung zu berücksichtigen – sowohl als Leistungsgegenstand als auch als Auswahlkriterium für den Dienstleister.

Schritt 4: Plan für den Ernstfall: Absolute Sicherheit gibt es nicht. Ein Unternehmen kann sich auf einen Hackerangriff vorbereiten, um im Ernstfall zum einen schnell reagieren zu können und zum anderen möglichst gut abgesichert zu sein. Ein solcher Plan wird am besten von Juristen, IT-Security-Spezialisten, dem technologischen Shopdienstleister und den Betriebsverantwortlichen in der Organisation gemeinsam entwickelt. Zusätzlich bietet beispielsweise die deutsche Versicherungswirtschaft sogenannte Cybersecurityversicherungen an, mit denen ein Anbieter das verbleibende Risiko und somit die geschäftliche Existenz absichern kann.

Cybersecurity: Jetzt angehen und in Zukunft profitieren

Die Augen vor den Gefahren verschließen und hoffen, dass alles gutgeht, scheint gemäß der Forsa-Umfrage en vogue zu sein. Wer allerdings online langfristig erfolgreich sein will, sollte Verantwortung übernehmen und seine Risiken abschätzen. Damit schützt ein Betreiber ebenso sich wie auch die eigenen Kunden und Partner. Die drastische Zunahme von Cybercrime und die inzwischen einfache Verfügbarkeit von Angriffshilfsmitteln verstärkt die Dringlichkeit des Handlungsbedarfs auf Seiten der Betreiber. Die eco-Studie zeigt auf, dass dieses Bewusstsein im Mittelstand ankommt – aber erst langsam. Den Herausforderungen müssen sich Betreiber von Webplattformen nicht alleine stellen: Mit Partnern, die die Problemstellungen und Risiken kennen und wissen, welche Cybersecurityfragen relevant sind, lässt sich jedes E-Commerce-Projekt sicher planen, umsetzen oder optimieren – am besten, bevor ein Schaden eingetreten ist.

Steffen Ritter arbeitet als E-Commerce Consultant und Software Architect bei AOE GmbH in Wiesbaden. In dieser Funktion berät er Kunden und erstellt Konzepte in den Bereichen Integrationen, Systemarchitekturen, Identity Management und IT-Security im Web in Digitalisierungs- und E-Commerce-Projekten. AOE entwickelt seit 20 Jahren erfolgreiche E-Commerce-Projekte und unterstützt seine Kunden im IT-Security-Umfeld besonders im Web-Application-Security-Bereich durch Analysen, Beratung, Konzepte, Penetrationstests und ähnliches wie auch bei der Konzeptionierung von OAuth-gestütztem IDM und SSO und deren Implementierung.

Links & Literatur

[1] https://www.gdv.de/resource/blob/61466/0456901217b39a5893bc6829b8d7d156/report-cyberrisiken-im-mittelstand-2020-data.pdf

[2] § 823 BGB: https://www.gesetze-im-internet.de/bgb/__823.html

[3] IT-Sicherheitsgesetz 2015: https://www.bgbl.de/xaver/bgbl/start.xav?startbk=Bundesanzeiger_BGBl&jumpTo=bgbl115s1324.pdf

[4] § 13 TMG Abs. 7: https://www.gesetze-im-internet.de/tmg/__13.html

[5] eco-Studie: https://www.eco.de/presse/immer-mehr-unternehmen-planen-fuer-den-it-notfall

[6] Gesetz gegen den unlauteren Wettbewerb: https://www.gesetze-im-internet.de/uwg_2004/index.html

[7] Telemediengesetz: https://www.gesetze-im-internet.de/tmg/index.html

[8] DSVGO im Original: https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32016R0679

[9] Preisangabenverordnung: https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32016R0679

[10] Gesetz über Urheberrecht und verwandte Schutzrechte: https://www.gesetze-im-internet.de/urhg/index.html