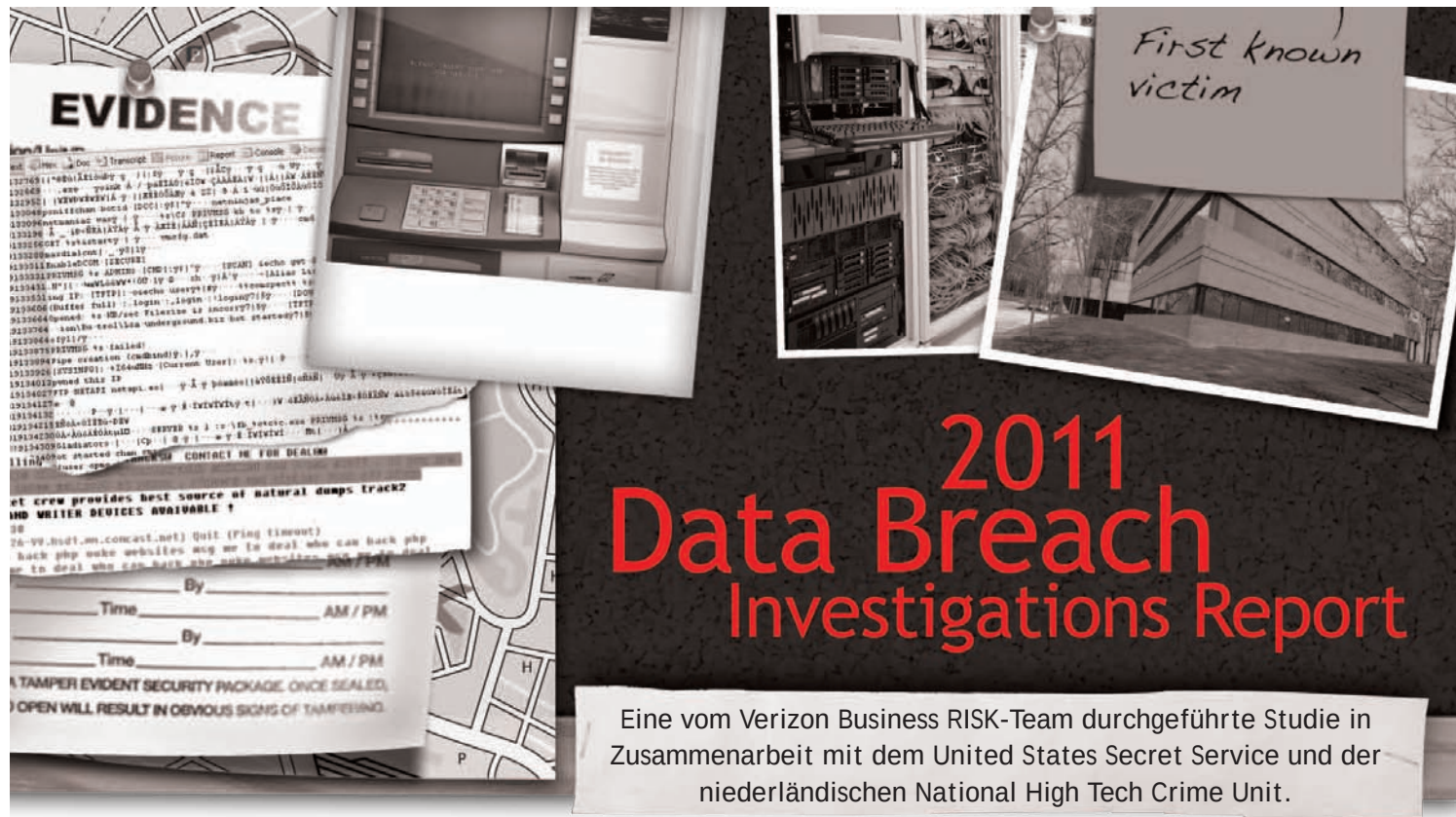




Executive Summary

361 Millionen >> 144 Millionen >> 4 Millionen. So lauten die Gesamtzahlen aller kompromittierten Datensätze, die von Verizon und dem United States Secret Service (USSS) innerhalb der letzten drei Jahre bearbeitet wurden. Nach vier Jahren mit einer steigenden Anzahl an Datenverlusten, die im Jahr 2008 mit rekordverdächtigen 361 Millionen ihren Spitzenwert erreichte, vermuteten wir, dass der Rückgang auf 144 Millionen im Jahr 2009 entweder Zufall oder ein Zeichen für die Zukunft war. Die Gesamtzahl von weniger als vier Millionen kompromittierten Datensätzen im Jahr 2010 scheint darauf hinzudeuten, dass es ein Zeichen war. Aber Zeichen wofür? Hält dieser Trend an oder handelt es sich um eine vorübergehende Tendenz?

Wir freuen uns, dass uns der United States Secret Service (USSS) im Data Breach Investigations Report (DBIR) für 2011 beim Beantworten dieser Fragen unterstützt. Außerdem dürfen wir die niederländische National High Tech Crime Unit (NHTCU) in unserem Team begrüßen. Diese Zusammenarbeit bot uns das Privileg – und die Herausforderung –, **seit unserem letzten Bericht rund 800 neue Fälle von Datenangriffen zu untersuchen** (darunter 761 für 2010). Setzen wir diese Zahl in ein Verhältnis: Die Verizon-USSS Datensätze von 2004 bis 2009 umfassen nur etwa 900 Verstöße. Wir haben die Größe unseres Datensatzes allein im Jahr 2010 nahezu verdoppelt!

Vom Forschungsstandpunkt aus gesehen, ist es interessant, dass die niedrigste Gesamtzahl an Datenverlusten im selben Jahr erfasst wurde, in dem auch die meisten Fälle aller Zeiten untersucht wurden. Es waren nicht nur die meisten Fälle, die wir je untersucht haben. Noch nie zuvor war die Vielfalt an Verursachern der Bedrohung, Bedrohungsszenarien, betroffener Assets und der entsprechenden Sicherheitsattribute so groß. Wir nahmen hochautomatisierte und erfolgreiche Angriffe von außen unter die Lupe, schwer erkennbare, schleichende Angriffe, komplexe interne Betrugsfälle, landesweite Schemata zum Angriff auf Geräte, Angriffe durch geschickte Ausnutzung sozialer Verhaltensweisen und vieles mehr. Einige der Rohstatistiken scheinen dieser Vielfalt zu widersprechen. So hat beispielsweise der Prozentsatz der externen Sicherheitsverletzungen mehr Schlagseite denn je. Allerdings ist hierbei die Änderung des Umfangs zu berücksichtigen. Zuvor stand „10 %“ für etwa 10 – 15 Sicherheitsverletzungen von durchschnittlich 100 – 150 Fällen pro Jahr. Jetzt bedeutet es 75 Sicherheitsverletzungen von allen im Jahr 2010 registrierten Fällen. Behalten Sie diese Tatsache im Hinterkopf, wenn Sie sich die Ergebnisse des aktuellen Berichts ansehen und analysieren.



POLITIE
• Korps landelijke politiediensten



Mit den von Verizon im Jahre 2010 bearbeiteten Fällen und den Daten des USSS und der NHTCU umfasst die DBIR-Reihe nun sieben Jahre mit mehr als 1700 Datenverletzungen und über 900 Millionen kompromittierten Datensätzen. Diese fortlaufende Untersuchung liefert uns wertvolle Informationen, und wir freuen uns, diese Ergebnisse erneut mit Ihnen teilen zu können. Unser Ziel besteht wie immer darin, unseren Lesern mit den in diesem Bericht dargestellten Daten und Analysen eine hilfreiche Richtlinie für Ihre Planungs- und Sicherheitsmaßnahmen bieten zu können. Hier zunächst wie immer einige Highlights:

Wer steckt hinter Datenverletzungen?

92 % externe Ursachen (+22 %)

17 % Insiders (-31 %)

<1 % Geschäftspartner (-10 %)

9 % mehrere Parteien (-18 %)

Falls Sie diese Zahlen über die Jahre hinweg verfolgt haben, denken Sie möglicherweise, dass wir unsere Fahne nach dem Wind hängen. Wir geben zu, dass im RISK-Team ratloses Kopfschütteln herrschte, als wir versuchten, diese Zahlen zu interpretieren. Im Jahr 2009 stieg die Zahl der Sicherheitsverletzungen durch Insider sprunghaft an, als wir die Daten von USSS integrierten. Allerdings ging 2010 die Zahl auch wieder zurück auf das Niveau vor der Integration der USSS-Daten, obwohl wir sie weiterhin berücksichtigten. Lesen Sie den Bericht, um alle Informationen darüber zu erhalten. Im Wesentlichen läuft es aber eher auf einen ENORMEN Anstieg kleinerer externer Angriffe als auf einen Rückgang der Angriffe durch Insider hinaus. Und der Rückgang der Sicherheitsverletzungen durch Partner setzte sich kontinuierlich fort.

Wie entstehen diese Datenverletzungen?

Aufgrund des geringeren Anteils interner Angriffe, hat Missbrauch seine Spitzenposition auf der Liste der Bedrohungskategorien verloren. Hacking und Malware haben erneut die Führung übernommen und sind gefährlicher als je zuvor. Fehlende, unzureichende und gestohlene Zugangsdaten geraten außer Kontrolle. Mit einem rasanten Zuwachs haben wir einen Newcomer unter den drei Bestplatzierten: physische Angriffe. Nachdem sich 2009 der Prozentsatz aller Sicherheitsverletzungen verdoppelt hatte, verdoppelte er sich 2010 erneut. Möglicherweise ist Cyberkriminalität immer weniger „cyber“? Trotz eines geringeren Anteils war die Anzahl von Missbräuchen und sozialer Manipulationen dennoch hoch und bot uns erstaunliche Beispiele für fehlerhaftes Verhalten, Betrug und Material für spannende Filmszenen.

50 % Hacking in irgendeiner Form (+10 %)

49 % Malware (+11 %)

29 % physische Angriffe (+14 %)

17 % Missbrauch von Zugriffsberechtigungen (-31 %)

11 % Social-Engineering-Taktiken (-17 %)

Welche Gemeinsamkeiten bestehen?

83 % Gelegenheitsziele (<>)

92 % waren nicht sehr komplex (+7 %)

76 % aller Datenverletzungen kamen von Servern (-22 %)

86 % wurden von einer dritten Partei entdeckt (+25 %)

96 % der Datenschutzlücken wären durch einfache oder intermediäre Kontrollen vermeidbar gewesen (<>)

89 % der Betroffenen hatten keine PCI DSS-Compliance erreicht (+10 %)

Unglücklicherweise bedarf es für Sicherheitsverletzungen in der Regel keiner hochkomplizierten Angriffe. Die meisten Angriffe richten sich auf Gelegenheitsziele und weniger auf speziell ausgewählte Ziele. Ein Großteil der Daten wird von Servern gestohlen und die Opfer bemerken häufig nichts von der Sicherheitsverletzung, bis ein Dritter sie benachrichtigt. Und fast alle Sicherheitsverletzungen sind vermeidbar (zumindest im Nachhinein) und zwar ohne komplizierte oder teure Lösungsmaßnahmen. An dieser Stelle würden wir wirklich gerne über bedeutende Veränderungen (d.h. negative Zahlen) berichten, aber unsere Ergebnisse lassen dies nicht zu.

Obwohl das nicht für alle von uns untersuchten Fälle zutrifft, ergaben die Untersuchungen, dass in Fällen, in denen die PCI-DSS galten, das Compliance-Niveau relativ niedrig war.

Obwohl wir alle noch so intensiv darüber nachdenken und wirklich gerne etwas Neues berichtet hätten, ist das einfach nicht möglich. Moment – das stimmt so nicht ganz. Wir möchten Unternehmen, die Kreditkartenlesegeräte besitzen oder verwalten (wie ATMs, Tankstellen, POS-Terminals und sonstige Kiosks) daran erinnern, diese regelmäßig auf Anzeichen für Manipulation und Skimming zu überprüfen. Solche Angriffe haben in den letzten Jahren zugenommen.

Gerne kochen wir bei Bedarf etwas Neues auf, aber die Punkte rechts (und im Abschnitt „Schlussfolgerungen und Empfehlungen“) sind sozusagen ein wesentlicher Bestandteil einer ausgewogenen Ernährung. Außerdem hat unsere Untersuchung 2010 ergeben, dass viele noch nicht davon gekostet haben, und es wäre unhöflich, den Tisch abzuräumen, bevor sie aufgegessen haben. Wenn Ihnen Fastfood lieber ist, finden Sie das an jeder Ecke.

Guten Appetit!

Worauf sollten sich die Präventionsmaßnahmen konzentrieren?

- ✓ Überflüssige Daten entfernen; die restlichen kontrollieren
- ✓ Sicherstellen, dass wesentliche Kontrollen durchgeführt werden
- ✓ Die oben genannten Punkte noch mal überprüfen
- ✓ Prüfung externer Zugangsdienste
- ✓ Webanwendungen testen und überarbeiten
- ✓ Benutzerkonten überwachen und Zugangsprivilegien kontrollieren
- ✓ Ereignisprotokolle überwachen
- ✓ ATMs und andere Kreditkartenlesegeräte auf Manipulation überprüfen

Jahresrückblick 2010

Cloud, Aurora, Mobility, Zeus, APT, Wikileaks, Stuxnet, Anonymous. Wenn man eine Wortwolke aus Infosec-Überschriften aus dem Jahr 2010 erstellt hätte, dann wären diese Begriffe sicher groß und fettgedruckt. Daraus ergibt sich eine interessante Gegenüberstellung von Themen. Während uns dank der Cloud und mobiler Geräte mehr und mehr alles von überall aus, mit jedem und jederzeit möglich ist, erinnern uns Aurora, Zeus, Advanced Persistent Threats (APTs), Wikileaks und Stuxnet daran, wie schwierig es ist, unsere Informationen in einer von Benutzerfreundlichkeit getriebenen Welt zu schützen. Da die Untersuchung unserer Fälle (und der von USSS und NHTCU) einen Blick in diese Welt eröffnen, könnte man erwarten, dass auch diese Aspekte in dem Jahresbericht zu den neuesten Trends bei Sicherheitsverletzungen behandelt werden. Und dieses Jahr erfüllt der DBIR diese Erwartungen.

Abgesehen von „Sicherheit“ war „Cloud“ das am häufigsten verwendete Wort bei den Präsentationstiteln auf der RSA Conference 2011. Es liegt uns allen definitiv sehr am Herzen. Aus diesem Grund werden wir häufig gefragt, ob „die Cloud“ in

Wir werden häufig gefragt, ob „die Cloud“ in vielen der von uns untersuchten Sicherheitsverletzungen eine Rolle spielt. Die einfache Antwort lautet: „Nein, nicht wirklich.“ Es geht weniger um Cloud-spezifische Themen, sondern vielmehr darum, dass wir die Kontrolle über unsere Assets und Daten verlieren und das damit verbundene Risiko ignorieren.

vielen der von uns untersuchten Sicherheitsverletzungen eine Rolle spielt. Diese Frage ist sowohl einfach als auch schwierig zu beantworten. Die einfache Antwort lautet: „Nein, nicht wirklich.“ Wir werden beispielsweise Sicherheitsverletzungen sehen, bei denen ein Hypervisor erfolgreich verwendet wird, der es dem Angreifer ermöglicht, auf virtuelle Maschinen (VMs) zuzugreifen. Andererseits liegen uns permanent Sicherheitsverletzungen vor, bei denen gehostete Systeme, Management Outsourcing, skrupellose Anbieter und sogar VMs involviert sind, obwohl die Angriffsformen nichts damit zu tun haben, ob es sich um eine VM handelt oder nicht. Kurz, es geht weniger um Cloud-spezifische Themen, sondern vielmehr darum, dass wir die Kontrolle über unsere Assets und Daten verlieren und das damit verbundene Risiko ignorieren.

Wenn wir gerade schon bei der Kontrolle unserer Assets und Daten sind, bietet es sich an, auch über mobile Geräte zu sprechen. Dies ist eine häufig gestellte Frage bei unseren Präsentationen und Diskussionen zum Thema Sicherheitsverletzungen. Tatsache ist, dass mobile Computing-Geräte (Tablets, Smartphones, Mobiltelefone usw.) in unseren Fällen nur selten die Ursache für Datenverlust sind. Es hat viel mit der Art der Fälle zu tun, die wir untersuchen. Wir konzentrieren uns eher auf vorsätzliche Sicherheitsverletzungen und Datenangriffe als auf versehentliches Verlieren von Geräten. Außerdem umfasst dieser Bericht nur bestätigte Datenangriffe. Die Bedrohungen für mobile Geräte sind real und wir rechnen damit, dass sie mit der Verwendung und den Anwendern steigen und sich verändern. Nehmen Sie als Beispiel die Auswirkung des iPads seit seiner Einführung vor

einem Jahr. Viele Führungskräfte, die sich zuvor nicht besonders für Technologie interessierten, fordern nun, bei der Arbeit iPads zu verwenden. Die Bequemlichkeit und Funktionalität dieser und ähnlicher Geräte wird deren Verbreitung in Unternehmen vorantreiben, und die Sicherheitsvorkehrungen müssen schnellstens daran angepasst werden.

Zeus ist bereits in unseren Fällen von 2009 aufgekeimt, entwickelte jedoch 2010 seine volle Blüte. Bei USSS und unserem Unternehmen wucherten Zeus und seine üblen Geschäftspartner namens Account-Übernahme und Transferbetrug bei Verbrauchern und Unternehmen gleichermaßen. Diese werden alle im Folgenden noch behandelt. Deshalb erwähnen wir sie hier nur kurz und fahren fort.

Wenn Zeus uns daran erinnert, dass Kriminelle es auf unser Geld abgesehen haben, dann erinnern uns Aurora, APTs, Stuxnet und Anonymous daran, dass einige Angreifer es auf mehr als nur das Geld abgesehen haben. Sie ließen das Informationsrisiko im Jahr 2010 für uns düsterer, zielgerichteter und persönlicher erscheinen (manche möchten vielleicht hoffnungslos hinzufügen). Egal, ob dieses Empfinden gerechtfertigt ist oder nicht, ein erheblicher Risikoanstieg ist schwer zu erkennen. Möglicherweise ist dieses Empfinden tatsächlich gerechtfertigt. Möglicherweise ist es auch nur für einige von uns gerechtfertigt. Möglicherweise hat sich das Risiko selbst gar nicht verändert, sondern lediglich unser Bewusstsein hat sich erheblich gewandelt. Möglicherweise handelt es sich um ein Körnchen Wahrheit, das von vielen Schichten Angst, Unsicherheit und Zweifel umgeben ist. Wir können mit Sicherheit sagen, dass unsere Untersuchung 2010 bestimmte Merkmale aufgedeckt hat, die man mit diesen Vorfällen in Verbindung bringen könnte. So haben zum Beispiel die Angriffe auf öffentliche Einrichtungen ein Rekordhoch erreicht. Wir untersuchten mehr Fälle als je zuvor, bei denen es um den Diebstahlklassifizierter Informationen, geistigen Eigentums und anderer Unternehmensdaten ging. Ist dies nur das vereinfachte Artefakt aus einer viel größeren und vielfältigeren Fallsammlung anstatt eine tatsächliche Veränderung? Vielleicht... vielleicht auch nicht.

APT's verdienen an dieser Stelle eine besondere Beachtung. Einige erinnern sich möglicherweise daran, dass wir bereits im DBIR 2010 unsere Bedenken geäußert haben, und an die darauffolgenden Blogbeiträge über die in der Sicherheits-Community ausgebrochene APT-Hysterie. Wir sind immer noch überzeugt, dass sich die Definition von APT schleichend ausweitete. Die Schöpfer des Begriffs verwenden ihn hauptsächlich in Bezug auf vom Staat veranlasste Angriffe in der Volksrepublik China. Andere wiederum bezeichnen damit jede Bedrohung, die überdurchschnittliche Fähigkeiten und Beharrlichkeit vorweist. Die logische Folge aus Ersterem ist die ernsthafte Bewertung von und die Auseinandersetzung mit dem Sicherheitszustand innerhalb von Regierungsbehörden und der industriellen Verteidigungsbasis (was nur mehr als recht ist). Die logische Schlussfolgerung aus Letzterem ist, dass man davon ausgehen muss, dass jeder zur Zielscheibe von APTs werden kann. Wobei es sich hier um einen Widerspruch in sich handelt, der irrationale Ängste vor dem Schreckgespenst hervorruft, während gewöhnliche Diebe Ihr Zuhause leerräumen. Es kann nicht jeder Ziel solcher Angriffe werden. Zweifellos stimmt es (belegt durch Ermittlungen), dass *einige* zum Ziel solcher vom Staat veranlassten Angriffe werden (in China oder woanders). Es stimmt zweifellos auch (ebenfalls belegt durch Erfahrung), dass *einige*, die denken sie wären ein Opfer von APTs, in Wirklichkeit Opfer von organisierten Verbrechern, Hacktivists, glorreichen Script Kiddies oder ihren eigenen Fehlern sind. Da APTs (gleich welcher Definition) real sind, wird es Zeit, dass wir endlich eine Definition festlegen und damit beginnen, uns zu verteidigen.

Sieht man von diesen Schlagzeilen ab, so hat sich im Jahr 2010 eine ganz andere Geschichte abgespielt. In den gesamten von Verizon und USSS untersuchten Fällen hat die Anzahl der Datensicherheitsverletzungen einen Tiefststand erreicht. DataLossDB, das Identity Theft Resource Center und weitere Quellen zeigen ebenfalls einen deutlichen Rückgang bei Datenverlusten oder Datenoffenlegungen. Was geht hier vor? Die Schlagzeilen klingen hoffnungsloser denn je, obwohl die Zahlen (zumindest einige) nahezu zuversichtlich stimmen. Warum solch ein Unterschied? Was trifft für 2010 wirklich zu? Wir sind der Meinung, dass in beiden Geschichten ein Quäntchen Wahrheit liegt. Wie oben erwähnt, haben die Schlagzeilen einen gewissen Wahrheitsgehalt. Genauso weisen die Zahlen im Zusammenhang mit Datenverlust auf mögliche und tatsächliche Veränderungen der Motive und Taktiken hin, die von Kriminellen zum Stehlen von Informationen verwendet werden. Wir haben uns bemüht, diese Geschichten und Statistiken in diesen Bericht einfließen zu lassen und ihre Kernbotschaften und ihre Bedeutung offenzulegen. Wir hoffen so einen kleinen Beitrag dazu zu leisten, dass 2011 und auch die folgenden Jahre besser enden.

Wenn Zeus uns daran erinnert, dass Kriminelle es auf unser Geld abgesehen haben, dann erinnern uns Aurora, APTs, Stuxnet und Anonymous daran, dass einige Angreifer es auf mehr als nur das Geld abgesehen haben. Sie ließen das Informationsrisiko im Jahr 2010 für uns düsterer, zielgerichteter und persönlicher erscheinen.

Schlussfolgerungen und Empfehlungen

Die Schlussfolgerung unseres letzten Berichts lautete:

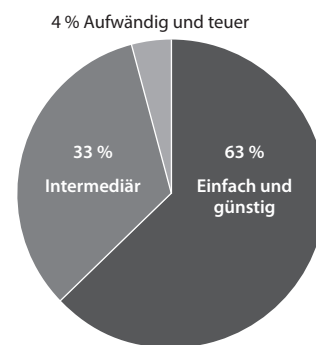
„Die Erstellung einer Liste von zuverlässigen Empfehlungen gestaltet sich mit jedem Jahr, in dem wir diesen Bericht veröffentlichen, schwieriger. Denken Sie darüber nach: Unsere Ergebnisse verändern und entwickeln sich mit der Zeit, doch selten sind sie völlig neu oder unerwartet. Warum sollten daher die Empfehlungen, die auf diesen Ergebnissen basieren, abweichen? Natürlich könnten wir improvisieren und eine lange Liste von Maßnahmen entwerfen, um eine Quote zu erfüllen, doch wir glauben, dass Sie das auch woanders bekommen können. Wir sind mehr an Qualität als an Quantität interessiert.“

Aber nachdem wir im letzten Jahr 800 weitere Fälle untersucht haben, sollten wir unzählige neue Empfehlungen für die Lösung Ihrer Sicherheitsprobleme haben, richtig? Nun, das ist in der Tat nicht der Fall. Die neuesten Beweise führen uns erneut zur gleichen Schlussfolgerung: Der Ursprung Ihrer Sicherheitsprobleme liegt nicht darin, dass es nichts Neues gibt (Abbildung 43 sieht aus wie immer). Es geht mit großer Wahrscheinlichkeit darum, dass bereits Vorhandenes, zu wenig oder falsch genutzt wird.

Dem mag man entgegensetzen, dass unsere Gegner clevere Betrüger sind, die bereit sind, sich anzupassen, um unsere „alte“ Verteidigung zu überwinden. Das stimmt (und wir haben dafür schon Beweise gesehen und besprochen), aber sehen wir das Ganze doch mal realistisch: Alles in allem betrachtet, glauben Sie, wir machen es ihnen wirklich schwer, sich anzupassen? Jahr für Jahr belegen die Zahlen, dass wir das nicht tun. Und das sollten wir ändern. Wenn sie sich anpassen, dann passen sie sich an. Das ist der Lauf der Dinge. Wir dürfen ihnen keine Gelegenheit geben, aus dem Stillstand Profit zu schlagen.

Zu diesem Zweck haben wir einige alte Rezepte herausgesucht, mit denen wir neuen Erfolg erzielen möchten. Wir haben die häufigsten Angriffe aus dem Jahr 2010 untersucht und fanden zutreffende Empfehlungen aus unseren früheren Berichten. Wir haben sie unten kategorisiert und aufgeführt und hoffen, dass Sie bei der Planung und am Verhandlungstisch davon profitieren können.

Abbildung 43. Kosten der empfohlenen präventiven Maßnahmen anhand des Prozentsatzes an Datenverletzungen*



* Nur von Verizon bearbeitete Fälle

Allgemeine Maßnahmen

Sorgen Sie für das Wesentliche und denken Sie erst dann über das Hervorragende nach: Wir stellen fest, dass viele Unternehmen in zahlreichen Bereichen ein sehr hohes Sicherheitsniveau erzielen, aber dafür andere Bereiche vernachlässigen. Kriminelle wählen in der Regel immer den Weg des geringsten Widerstands. Eine erfolgreiche Strategie gegen reale Angriffe sieht folgendermaßen aus: Entscheiden Sie sich zunächst für wichtige Kontrollinstrumente und stellen Sie die unternehmensweite Implementierung sicher - ohne Ausnahme. Danach können Sie sich bei Bedarf erweiterten Kontrollinstrumenten widmen.

Dem ist entgegenzusetzen, dass unsere Gegner clevere Betrüger sind, die bereit sind, sich anzupassen, um unsere „alte“ Verteidigung zu überwinden. Das stimmt (und wir haben dafür schon Beweise gesehen und besprochen), aber sehen wir das Ganze doch mal realistisch: Alles in allem betrachtet, glauben Sie, wir machen es ihnen wirklich schwer, sich anzupassen?

Zugangskontrolle

Ändern der Standardzugangsdaten: Einfach und effektiv: Sobald Ihre System-/Netzwerkadministratoren ein neues System errichten, ändern Sie das Passwort. Falls Sie diese Arbeiten an einen Drittanbieter übergeben, stellen Sie sicher, dass dieser das Passwort ändert. Gehen Sie nicht davon aus, dass Ihre Mitarbeiter oder Partner sich durchweg an alle Richtlinien und Verfahren halten. Neben dem Ändern der Standardzugangsdaten sollten Unternehmen sicherstellen, dass Passwörter einzigartig sind und nicht von mehreren Benutzern oder für verschiedene Systeme verwendet werden. Dies erweist sich vor allem bei Assets als problematisch, die von Drittanbietern gemanagt werden.

Jedes Jahr bietet sich uns bei der Untersuchung von Bedrohungsszenarien das gleich Bild: Die meisten Opfer werden nicht von unbekannten und unaufhaltsamen Angriffen überwältigt. In den meisten Fällen wissen wir genug über diese Angriffe und wir wissen auch, wie wir sie abwehren können.

Überprüfung der Benutzerkonten: Frühere Data Breach-Berichte und jahrelange Erfahrung machten uns klar, wie wichtig eine regelmäßige Überprüfung der Benutzerkonten ist. Diese Überprüfung sollte durch ein formelles Verfahren erfolgen, um sicherzustellen, dass aktive Konten gültig, erforderlich und richtig konfiguriert sind sowie über die entsprechenden (vorzugsweise wenige) Privilegien verfügen.

Privilegien von Nutzern einschränken und überwachen: Vertrauen ist gut. Kontrolle ist besser. Überprüfen Sie neue Mitarbeiter, um das Problem zu beseitigen, bevor es auftritt. Geben Sie Benutzern nicht mehr Privilegien, als diese benötigen (dies ist ein sehr wichtiger Punkt), und grenzen Sie Aufgaben klar voneinander ab. Stellen Sie sicher, dass sie angeleitet (über Richtlinien und Erwartungen) und überwacht werden (um sicherzugehen, dass sie sich daran halten). Privilegien sollten protokolliert werden und Meldungen an das Management beinhalten. Unvorgesehener Einsatz von Privilegien sollte Warnmeldungen erzeugen und untersucht werden.

Network Management

Sichere Remote-Zugangsdienste: In vielen Fällen wurden Remote-Zugangsdienste aktiviert und sind mit dem Internet verknüpft. Wir empfehlen, diese Services so einzurichten, dass nur spezifische IP-Adressen oder Netzwerke darauf zugreifen können. Außerdem ist es wichtig, den Zugriff auf sensible Systeme innerhalb des Netzwerks einzuschränken. In vielen Unternehmen kann mit jedem Gerät im Netzwerk eine Verbindung hergestellt und per Fernzugriff auf andere Geräte zugegriffen werden. Wir raten dringend von dieser Art der Geräteverwaltung ab. Schränken Sie externe Zugangsdienste auf spezifische Managementnetzwerk mithilfe von Zugriffskontrolllisten ein.

Ausgehenden Netzwerkdatenverkehr überwachen und filtern: An einem gewissen Punkt vieler Datenverletzungen gelangt etwas (Daten, Kommunikationen, Verbindungen) nach draußen, das bei entsprechender Prävention die Kette durchbrochen und den Datenverlust verhindert hätte. Durch die Überwachung, Kenntnis und Kontrolle des ausgehenden Datenverkehrs kann ein Unternehmen böswillige Aktivitäten deutlich reduzieren.

Sichere Entwicklung

Anwendungen testen und Code prüfen: SQL Injection, Cross-Site-Scripting, Authentifizierungsumgehung und Missbrauch von Session-Variablen machen fast die Hälfte der Angriffe durch Hacking oder unerlaubtes Eindringen in das Netzwerk aus. Es ist kein Geheimnis, dass die Angreifer immer tiefer in unsere Systeme eindringen und es nun auch auf die Anwendungsebene abgesehen haben. Warum ziehen unsere Verteidigungsstrategien nicht nach? Wie in allen anderen Bereichen gilt auch hier: Zunächst müssen die Brände gelöscht werden. Sogar simple Webanwendungen zum Scannen und Testen hätten viele der Probleme aufdecken können, die zu den schwerwiegendsten Sicherheitsverletzungen im letzten Jahr führten. Desweiteren sollten die Architektur, die Privilegien und der Quellcode regelmäßig überprüft werden. Auch ist die Implementierung eines Security Development Life-Cycle (SDLC)-Ansatzes für die Anwendungsentwicklung empfehlenswert. Und unterstützen Sie Ihre Entwickler dabei, sichere Codes schätzen zu lernen und zu programmieren.

Protokollmanagement und -analyse

Aktivieren Sie Protokolle für Anwendungen und Netzwerk und überwachen Sie diese: Nur allzu oft lagen den Opfern klare Hinweise auf Ereignisse vor, die zu den Sicherheitsverletzungen führten, allerdings wurden sie weder erkannt, noch wurde darauf reagiert. Prozesse zur vernünftigen, effizienten und effektiven Überwachung und entsprechendes Reagieren sind beim Datenschutz unerlässlich.

Beschränken Sie Ihre Protokolle jedoch nicht auf Netzwerk, Betriebssystem, IDS und Firewall. Berücksichtigen Sie auch Remote-Zugangsdienste, Webanwendungen, Datenbanken und andere wichtige Anwendungen. Diese können nützliche Daten zum Erkennen, Vorbeugen und Untersuchen von Sicherheitsverletzungen liefern.

Definieren Sie „verdächtig“ und „anormal“ (und suchen Sie dann danach): Das ist in der Tat etwas vage, aber eine Verallgemeinerung dessen, was alles damit verbunden ist, nur um eine Definition für jeden zu finden, wäre kontraproduktiv. Finden Sie heraus, was wichtig ist, erkennen Sie „normales Verhalten“ und erstellen Sie dann Mechanismen, mit denen Sie nach Abweichungen Ausschau halten können und die eine Warnmeldung generieren.

Ändern Sie Ihre Vorgehensweise bei der Ereignisüberwachung und Protokollanalyse: Basierend auf den Daten, die wir zum Zeitpunkt der Sicherheitsverletzung sammeln, sind wir der Meinung, dass Unternehmen sich besser weniger auf die „Echtzeit“-Methoden zum Erkennen von Sicherheitsverletzungen konzentrieren sollten, sondern eher auf die Methoden zur Erkennung der "Sicherheitsverletzungen der Woche". Wenn wir den Zeitraum zwischen Sicherheitsverletzung und Entdeckung von Wochen und Monaten auf Tage verkürzen könnten, dann würde der Schaden für Ihr Unternehmen erheblich reduziert werden. Konzentrieren Sie sich auf die offensichtlichen Dinge anstatt auf die kleinen Details. Dies muss nicht teuer sein. Ein einfaches Skript, um Protokollzeilen/-längen zu zählen und eine Benachrichtigung bei Vorfällen außerhalb des Toleranzbereichs zu senden, kann sich als sehr effektiv erweisen. Wir sind uns sicher, dass diese Vorgehensweise einen großen Nutzen verspricht und Zeit, Aufwand und Geld spart.

Schulung und Bewusstsein

Das Bewusstsein für Social Engineering stärken: Informieren Sie Ihre Mitarbeiter über die verschiedenen Arten des Social Engineering und von wo aus diese Angriffe erfolgen können. In vielen Fällen klicken Benutzer auf Links, auf die sie nicht klicken sollten, oder sie öffnen Anhänge von unbekannten Absendern. Honorieren Sie das Melden von verdächtigen E-Mails und Websites und geben Sie entsprechende Anreize für mehr Wachsamkeit.

Schulen Sie Mitarbeiter und Kunden für die Suche nach Anzeichen für Manipulation und Betrug: Solche Kampagnen gibt es in einigen Bereichen bereits seit einer Weile. Dennoch nimmt die Manipulation/der Betrug bei ATM und Kreditkartenlesegeräten zu – und zwar sowohl hinsichtlich der Anzahl als auch des Ausmaßes. Unternehmen, die solche Geräte besitzen, sollten diese regelmäßig untersuchen. Zusätzlich sollten Sie den Kunden zeigen, wie sie sich selbst schützen und dem Unternehmen beim Aufdecken potenzieller Probleme helfen können.

Management bei Zwischenfällen

Entwickeln Sie einen Plan zur Reaktion auf Zwischenfälle: Wenn eine Sicherheitsverletzung befürchtet wird, muss das Unternehmen bereit sein zu reagieren. Mit einem effektiven Plan zur Reaktion auf Zwischenfälle wird der Umfang der Sicherheitsverletzung reduziert und sichergestellt, dass die notwendigen Beweise gesammelt werden.

Trainieren Sie Ihre Mitarbeiter mit simulierten Zwischenfällen: Immerhin reden wir hier nur von Übung, keinem echten Ereignis, sondern lediglich von Übung für ein solches Ereignis (die Sportsfreunde unter Ihnen werden diesen Bezug möglicherweise verstehen). Ja, wir sprechen von Übung, denn erst durch Übung wird man zum Meister. Um effizient handeln zu können, sollten Unternehmen ein Routinetraining zur Reaktion auf Zwischenfälle absolvieren, das Reaktionsstrategien, die Erkennung und Einstufung von Bedrohungen, die Definition von Prozessen, den richtigen Umgang mit Beweisen und Simulationen umfasst.

Die gemeinsame Datennutzung

Eine der wichtigsten und schwierigsten Herausforderungen beim Managen von Informationsrisiken ist das Fehlen von Daten. Als Führungs- und Fachkräfte einer Community stehen uns nur wenige Daten zur Verfügung, da wir sie nicht gemeinsam nutzen. Dafür gibt es viele Gründe, aber hauptsächlich sind es Zweifel, ob das auf eine praktische, sichere und für alle Beteiligten gewinnbringende Art und Weise möglich ist. Wir würden diesen Bericht gerne als Beispiel dafür sehen, dass sensible und nützliche Daten verantwortungsbewusst mit anderen geteilt werden können, damit möglichst viele davon profitieren. In den letzten beiden Jahren haben auch einige andere investigative Unternehmen ihre Ergebnisse veröffentlicht und wir begrüßen diese Ansätze. Jeder noch so kleine Beitrag hilft. Es wäre großartig, wenn andere Unternehmen auch teilnehmen würden. Und wenn Sie Ihre Ergebnisse über VERIS berichten würden, dann könnten wir Äpfel mit Äpfeln vergleichen. Wir helfen gerne wo immer wir können.

Außerdem würden wir auch gerne andere Unternehmen dazu einladen, die [VERIS Community Website](https://www2.icsalabs.com/veris/)¹² zu nutzen, um anonym Sicherheitsvorfälle aller Art (nicht nur Datenschutzverletzungen) zu berichten. Alle Ergebnisse (gesammelte und anonyme) sind für die Community frei zugänglich. Wenn Sie Informationen zu Ihren Zwischenfällen preisgeben, dann leisten Sie einen Beitrag zum gemeinsamen Wissen der Community und erhalten Zugriff auf den VERIS-Datensatz. Ziel ist es, eine Grundlage zu schaffen, mit deren Hilfe wir konstruktiv und kooperativ aus unseren Erfahrungen lernen und Risiken besser kontrollieren können.

Wir wissen, dass Zeit stets ein knappes Gut ist. Deshalb möchten wir Ihnen danken, dass Sie sich die Zeit genommen haben, diesen Bericht zu lesen.

¹² <https://www2.icsalabs.com/veris/> (Website in englischer Sprache)

verizonbusiness.com/de

verizonbusiness.com/de/socialmedia

verizonbusiness.com/thinkforward (Website auf Englisch)

© 2011 Verizon. Alle Rechte vorbehalten. MC14949 04/11. Die Namen und Logos Verizon und Verizon Business sowie sonstige Namen, Logos und Slogans, die auf Produkte und Dienstleistungen von Verizon verweisen, sind Marken oder Dienstleistungsmarken der Verizon Trademark Services LLC oder ihrer Tochtergesellschaften in den USA und/oder anderen Ländern. Sämtliche anderen erwähnten Marken und Dienstleistungsmarken sind Eigentum der jeweiligen Rechteinhaber.