**Betreff: BitSight Kommentar: Bluekeep Anfälligkeit und Patch-Rate nach Ländern sowie Branchen weltweit**

Sehr geehrte Damen und Herren,

wie bei EternalBlue (in 2017 ausgenutzt durch WannaCry) weist Microsoft auch bei Bluekeep auf die großen Risiken hin, die durch die Sicherheitslücke verursacht werden, und stellt einen Patch bereit. Der Patch wird jedoch länder- und branchenabhängig recht unterschiedlich ausgerollt.

In der folgenden Dateneinsicht stellt [BitSight](https://www.bitsight.com/) mit der Dateneinsicht zur Windows-Schwachstelle Bluekeep (CVE-2019-0708) Details zur Bluekeep Anfälligkeit sowie zur Patch-Rate vor und nennt Gegenmaßnahmen, die Organisationen ergreifen können.

Wenn Sie Fragen haben oder an einem Interview bzw. Fachartikel interessiert sind, melden Sie sich gerne jederzeit!

**Bluekeep Anfälligkeit und Patch-Rate nach Ländern sowie Branchen weltweit**

*Von Patrick Steinmetz, DACH Sales, BitSight*.

BitSight ist Anbieter von IT-Sicherheitsratings und betreibt über seine Tochterfirma AnubisNetworks das weltweit größte Sinkhole.

Im Zusammenhang mit seinem Geschäftsmodell sammelt BitSight seit dem 31. Mai Informationen über die Exposition und den Sicherheitsstatus der Systeme, die sich in Unternehmensnetzwerken befinden und für Bluekeep anfällig sind.

BitSight hat das Tool von Robert Graham in seine eigene Scan-Plattform integriert, um kontinuierlich nach anfälligen Systemen zu suchen, und kann die von Robert Graham veröffentlichten Zahlen bestätigen: Weltweit hat BitSight fast eine Millionen Computer mit Internetzugang gefunden, die für die Schwachstelle Bluekeep anfällig sind.



Systeme mit extern exponiertem RDP, aber mit aktivierter Network Level Authentication (NLA) waren schon vor der Veröffentlichung des Patches nicht anfällig und bleiben geschützt.

BitSight hat die Anfälligkeit für Bluekeep auch nach Ländern aufgeschlüsselt. Die folgende Grafik zeigt die 15 Länder mit der größten Gesamtzahl an Rechnern, die für die Schwachstelle gefährdet waren, aber bereits gepatcht wurden (blau) und weiterhin gefährdeten, ungepatchten Systemen (rot). Systeme mit aktivierter NLA werden hier nicht mitgezählt.



Die folgende Grafik setzt die Anzahl der gefährdeten Systeme (ohne NLA) mit der Anzahl der gepatchten Systeme ins Verhältnis. Da Länder mit sehr geringer Exposition verzerrte Ergebnisse liefern könnten, sind Länder mit weniger als 20.000 exponierten RDP Hosts herausgefiltert.



Die IT-Verantwortlichen in den verschiedenen Ländern haben demnach sehr unterschiedlich auf den Patch-Bedarf ihrer Systeme reagiert. Deutschland ist erfreulicherweise gut aufgestellt: Die überwiegende Zahl der Rechner wurde bereits gepatcht. Insgesamt zählte BitSight hierzulande nur 110.993 Systeme, die sich in Unternehmensnetzwerken befinden und ohne den Patch für Bluekeep anfällig gewesen wären. Davon wurden bereits 94.719 Stück gepatcht, 16.274 waren demnach zum Zeitpunkt der Erstellung des Artikels noch gefährdet. Auch die USA, Frankreich, Japan, die Niederlande und Großbritannien schneiden gut ab.

BitSight hat ebenso die Anfälligkeit von Branchen auf Bluekeep analysiert. Die folgende Tabelle zeigt den Anteil der Unternehmen einer Branche, bei denen BitSight mindestens ein gefährdetes System gefunden hat; bei denen der Patch bereits auf alle über das Internet erreichbare Computer aufgespielt wurde oder wo die Rechner durch eine zusätzliche Authentifizierungsmaßnahme (NLA) geschützt sind; sowie Unternehmen, die nicht für Angriffe über RDP anfällig sind.



Unternehmen aus den Bereichen Telekommunikation, Bildung und Technologie sind am stärksten betroffen. Telekommunikationsunternehmen hosten aber in der Regel Systeme für ihre Endkunden, die sie selbst nicht aktualisieren können, was die höhere Quote für diese Branche erklärt.

**EternalBlue versus Bluekeep**

Basierend auf den Daten, die BitSight seit Anfang Mai gesammelt hat, und den historischen Daten, die BitSight für 2017 vorliegen, lässt sich die Anzahl der exponierten Systeme unmittelbar vor dem Erkennen der Sicherheitslücke und der Bereitstellung des Patches durch Microsoft vergleichen. EternalBlue war der Bug, der vom WannaCry Wurm ausgenutzt wurde. WannaCry trat etwa zwei Monate nach der Warnung vor EternalBlue und der Bereistellung des Patches durch Microsoft dafür auf.



Die Grafik zeigt die potenzielle Exposition um das Datum herum, an dem die Bugs bekannt gegeben wurden, ohne Berücksichtigung von Patching. BitSight berechnet das potenzielle Risiko für EternalBlue, indem die Anzahl der SMBv1 Hosts gezählt wurde, die im April 2017 über das Internet erreichbar waren. Für Bluekeep hat BitSight die Anzahl der erreichbaren Hosts mit RDP und deaktivierter NLA im Mai 2019 gezählt.

Die Situation ist bezüglich der Anzahl der exponierten Systemen vergleichbar. Bluekeep betrifft zum Zeitpunkt der Bug-Bekanntgabe und Patch-Freigabe nur eine etwas größere Anzahl an Systemen.

Bei der Verfügbarkeit von Exploits ist die Situation anders. Im Fall der EternalBlue Schwachstelle ist fast zeitgleich mit dem freigegebenen Patch ein zuverlässiger Exploit durchgesickert. Für Bluekeep gibt es zum Zeitpunkt dieses Artikels keinen allgemein verfügbaren Exploit, nur mehrere Berichte über Proof-of-Concept-Exploits, die leicht durch Reverse Engineering des Patches erstellt werden konnten.

Auf jeden Fall ist das zerstörerische Potenzial ähnlich oder schlimmer als bei WannaCry, insbesondere wenn Patch-Management nicht ernst genommen wird.

**Emfehlungen für Unternehmen**

Die [National Security Agency (NSA) empfiehlt folgende Maßnahmen](https://www.nsa.gov/News-Features/News-Stories/Article-View/Article/1865726/nsa-cybersecurity-advisory-patch-remote-desktop-services-on-legacy-versions-of/), um die Widerstandsfähigkeit gegen Bluekeep zu erhöhen, während große Netzwerke gepatcht und upgegraded werden:

* Blockieren des TCP Ports 3389 über die Firewalls, insbesondere an allen Firewalls, die über dasd Internet erreichbar sind. Dieser Port wird im RDP-Protokoll verwendet und durch die Blockierung werden Versuche unterbunden, eine Verbindung herzustellen.
* NLA aktivieren. Diese Sicherheitsverbesserung erfordert, dass Angreifer über gültige Anmeldeinformationen verfügen, um eine Remote Code Authentication durchzuführen.
* Deaktivieren von Remote Desktop Services, wenn sie nicht benötigt werden. Die Deaktivierung nicht genutzter und nicht benötigter Dienste trägt dazu bei, die Gefährdung durch Sicherheitsschwachstellen insgesamt zu verringern und ist eine bewährte Vorgehensweise, auch abseits der BlueKeep-Bedrohung.

**Zur BitSight Technologie**

IT-Sicherheitsratings von BitSight verfolgen folgenden Ansatz: automatisches Sammeln und Auswerten großer Datenmengen im Hinblick auf IT-Sicherheit. Die datenbasierte, kontinuierliche Messung der IT-Sicherheit und automatisierte Auswertung durch leistungsfähige Algorithmen ermöglicht einen tagesaktuellen Überblick von außen über die Cybersicherheitsleistungen Organisationen – eine stets aktuelle Bewertung der Cybersicherheitsleistung von hunderttausenden Organisationen. Dabei steht vom generellen Überblick über beispielsweise die deutschlandweite Cybersicherheitsleistung bis hin zu kleinsten Details wie offenen Ports und Malware-Infektionen einzelner Computer immer genau die Information bereit, die benötigt wird.

BitSight hat mehr als 1.500 Kunden weltweit, dazu gehören unter anderem BNP Paribas, PwC, KPMG, Mondelēz, Bertelsmann und Burberry.